Acta Math. Hung.
56 (3—4) (1990), 309—324.

ON A PROBLEM OF R. PÖSCHEL ON LOCALLY INVERTIBLE MONOIDS

I. SZALKAI (Veszprém)

To the memory of my Parents

0. Introduction and statement of results

Automorphisms of algebraic structures have been widely investigated. In connection with the characterzation of properties of endomorphism monoids, in [$P1$] it was formulated a problem which we are going to investigate with a set-theoretic approach.

Before formulating the set theoretic version of the problem we need a few definitions:

DEFINITION 0.0 (i) For sets A and B denote by ${}^B A$ the set of functions mapping from B to A and the set of permutations on A by S_A.

(ii) $\circ$ and $\restriction$ denote the operations of composition and restriction respectively. (That is for $f, g \in {}^A A$, $D \subset A$ and $b \in A$ $(f \circ g)(b) = f(g(b))$, $f \restriction D \in {}^D A$ and for every $d \in D$ $(f \restriction D)(d) = f(d)$.) Let further $f''D = \mathrm{Range}\,(f \restriction D)$ for $f \in {}^B A$ and $D \subset \mathrm{Range}\,(f)$

(iii) a monoid $M \subset {}^A A$ is called *locally invertible* iff for every $f \in M$ and finite subset D of A there is a $g \in M$ such that $(g \circ f) \restriction D = \mathrm{id}$.

(iv) for $F \subset {}^A A$ let $\mathrm{Loc}\,(F) = \{f \in {}^A A\colon \forall D \subset A,\ D$ finite, $\exists g \in F\ f \restriction D = g \restriction D\}$ the *local closure* of F.

Then the problem is whether the following statement is true:

$P(A)$ = "$M \subset \mathrm{Loc}\,(S_A \cap \mathrm{Loc}\,(M))$ holds for every locally invertible monoid $M \subset {}^A A$."

We denote the negation of $P(A)$ by $\neg P(A)$.

REMARKS. (a) R. Pöschel raised the problem in Szeged, 1983 (see [C, p. 653]). The problem first appeared in [P3], the original problem is whether "a clone of relations closed with respect to complementation" is an equivalent definition of Krasner clones of 2^{nd} kind. (For more algebraic background and intuition see [P1, p. 161] or [P2].)

(b) Stone's definition in [St, p. 41] is, in fact, equivalent to (iii).

The validity of $P(A)$ depends on the cardinality of A. It is easy to see that for cardinal numbers $\lambda < \varkappa$ $P(\varkappa)$ implies $P(\lambda)$. (If A is finite then $P(A)$ is trivially true.) The affirmative answer for countable A was first given by J. Kollár (see eg. [P1, p. 164]) and the reader can make up a proof himself also for this case.

Our results are the following (for the definitions of CH or MA see [K]):

THEOREM 2.1. CH *implies* $\neg P(2^{\aleph_0})$.

THEOREM 3.1. (a) MA *(Martin's axiom) implies* $\neg P(2^{\aleph_0})$.
(b) MA (λ) *implies* $P(\lambda)$ *for* $\lambda < 2^{\aleph_0}$ *for countable monoids* M.

THEOREM 3.2. $2^{\aleph_0} = 2^{\aleph_1} = \aleph_2 + \neg\mathrm{MA} + \neg P(2^{\aleph_0})$ *is relative consistent with* ZFC.

THEOREM 3.4. $2^\lambda=\lambda^+$ *implies* $\neg P(2^\lambda)$ *for any cardinal* λ.

(The same argument shows $\neg P(\varkappa)$ for any $\varkappa$ if $2^\lambda \leqq \varkappa$ for every $\lambda<\varkappa$.

It remains open whether $\neg P(2^{\aleph_0})$ follows from ZFC or $P(2^{\aleph_0})$ is consistent. Further, very little is known about $P(\lambda)$ for $\aleph_0<\lambda<2^{\aleph_0}$.

Though Theorem 3.4 generalises all the other theorems, we prove it at the end because of the following reason. Theorem 3.1 (b) shows that the cardinality of the monoid plays an important role and in the proof of Theorem 3.4 we construct a monoid of size λ while the other proofs (using slightly different arguments) give countable monoids. Theorem 3.1.b shows that countable counterexamples can not be given in ZFC alone.

In Section 1 we prove Lemma 1.2 which is the key to our results. In Section 2 we prove our main result: Theorem 2.1. Using the same ideas (but forcing techniques) we prove generalizations of this theorem (Theorems 3.1, 3.2 and 3.4). The author thanks R. Pöschel, P. Komjáth and P. Prőhle for helpful discussions.

1. The Lemma

In this Section we prove a lemma which is the starting point of our proofs and introduce some useful definitions which throw some light to the behaviour of our monoids.

We start with the notations and definitions we need. ω_0 is the set $\{0, 1, 2, \ldots\}$ and $k<\omega_0$ means $k\in\omega_0$ and $i<k$ means $i\in\{0, 1, \ldots, k-1\}$ for $k\in\omega_0$.

DEFINITION 1.0. (i) $M\subset {}^AA$ is a *free monoid* iff it has no nontrivial $\circ$-equations. (That is for every $f_1, f_2, f_3, f_4 \in M$ if $f_1\circ f_2=f_3\circ f_4$ then there are $g_j\in M$ ($j=1, 2, \ldots, n$ for some $n<\omega_0$) such that $f_1=g_1\circ\ldots\circ g_k$, $f_2=g_{k+1}\circ\ldots\circ g_p$ and $f_3=g_1\circ\ldots\circ g_l$, $f_4=g_{l+1}\circ\ldots\circ g_n$ for some $k, l<n$.)

(ii) For a one-to-one function $f\in {}^AA$ we denote by f^{-1} the partial inverse of f: $\mathrm{Dom}(f^{-1})=\mathrm{Range}(f)$ and $f^{-1}(a)=b$ iff $f(b)=a$ for $a\in\mathrm{Dom}(f^{-1})$.

(iii) For a set $F\in {}^AA$ we denote by $\langle F, \circ\rangle$ ($\langle F, \circ, -1\rangle$) the set of functions generated from F with the help of operation $\circ$, the composition (with the help of $\circ$ and -1, the partial inverse, resp.). (To be more precise, $g\in\langle F, \circ\rangle$ and $h\in\langle F, \circ, -1)$ iff there are $k\in\omega_0$, $f_1, \ldots, f_k\in F$ and $\varepsilon_1, \ldots, \varepsilon_k\in\{+1, -1\}$ such that $g=f_1\circ\ldots\circ f_k$ and $h=f_1^{\varepsilon_1}\circ\ldots f_k^{\varepsilon_k}$ where we write f^{+1} for f and f^{-1} for the partial inverse of f.) (Sometimes we write f^0 for id.)

(iv) A monoid $M\subset {}^AA$ is finitely generated iff there is $F\subset M$ finite such that $M=\langle F, \circ\rangle$.

In the next section we extend the elements of the monoid $M\subset {}^AA$ (constructed in this section) to $N\subset {}^BB$, $B\supset A$ $M=\{f\restriction A: f\in N\}$. In the meantime we want to "kill" (every) permutation $\pi\in\mathrm{Loc}(M)\cap S_A-\{\mathrm{id}_A\}$, that is $\pi\neq\varrho\restriction A$ for all $\varrho\in\mathrm{Loc}(N)\cap S_B$. To achieve this, while extending the elements of M to B, we have to extend their local inverses in such a way that the partially killed π will not rise again. This is ensured by requiring the existence of local inverses for all $f\in M$ with good properties (and Lemma 1.2 (iv); for further details see the sets E_i and Lemma 2.2). These good properties are declared in the following definition. (Any of the finite sets may be empty.)

DEFINITION 1.1 (weaker version). A set of functions $F\subset {}^AA$ (A is an arbitrary set) is called *fairly complete* iff:

FOR EVERY $f\in F$, $D\subset A$ finite, $v<\omega$, $D_m\subset A$ finite and one-to-one function g_m mapping from D_m to A, $g_m\neq \mathrm{id}\restriction D_m$ and $\mathscr{H}\subset F$ finite such that $\varphi\restriction D_m\neq g_m$ for all $\varphi\in\langle\mathscr{H}_m, \circ, -1\rangle$ and $m<V$, THERE ARE infinitely many $t\in F$ such that $t\circ f\restriction D=$ $=\mathrm{id}\restriction D$ and for every $m<v$ and every $\psi\in\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$ we have $\psi\restriction D_m\neq g_m$ for $m<v$.

Roughly speaking t is a local inverse for $f\restriction D$ and moreover makes no forbidden functions in $\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$ with respect to g_m simultaneously for $m<v$.

(In the construction of the next section, one of the g's is will be the permutation π to be killed, see also Lemma 2.2.)

Observe that if F is fairly complete then it is locally invertible. Further if F is locally invertible (fairly complete) then so is $\langle F, \circ\rangle$ too.

However, in proving Theorem 2.1 (see Case 3 in Claim 2.3) we need a stronger property:

DEFINITION 1.1 (stronger version). A set of functions $F\subset {}^AA$ (A is an arbitrary set) is caled *strongly fairly complete* iff:

FOR EVERY $f\in F$, $D\subset A$ finite, $v<\omega_0$, $D_m\subset A$ finite and one-to-one function g_m, mapping from D_m to A, $g_m\neq\mathrm{id}\restriction D_m$ and $\mathscr{H}_m\subset F$ finite for $m<v$, THERE ARE infinitely many $t\in F$ such that $t\circ f\restriction D=\mathrm{id}\restriction D$ and for every $m<v$ and every $\psi\in\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$ $\psi\restriction D=g_m$ implies $D\subset\mathrm{Dom}(\psi')$ and $\psi'\restriction D_m=\psi\restriction D_m$ where ψ' results if we replace t^{-1} by $(f\restriction D)^{-1}$ (and t^{-1} by $f\restriction D$) in ψ everywhere.

We need this stronger version because in the main construction (see the proof of Claim 2.3) we can not ensure that $\psi\restriction D_m\neq g_m$ for all $\psi\in\langle\mathscr{H}_m, \circ, -1\rangle$ but for ψ' only if ψ' is defined as above.

In what follows we always use the stronger version of Definition 1.1.

The following lemma is the key to our results:

LEMMA 1.2. *There exists a countable monoid* $M\subset {}^AA$ *on a countable set* A *with the following properties:*

(i) *M is not finitely generated and has independent* $\circ$ — *generators* $F=\{f_i\colon i<\omega_0\}$,

(ii) *F is strongly fairly complete,*

(iii) $\mathrm{Loc}\,(\langle\{f_i\colon i<j\}, \circ, -1\rangle)\cap S_A\subseteqq\{\mathrm{id}_A\}$ *for every* $j<\omega_0$.

REMARKS M is free by (i) and locally invertible by (ii). We will use (iii) in the next section to construct some sets E_j for $j<\omega_0$. Using their properties and the fairly completeness of M we will be able to kill $\pi\in\mathrm{Loc}\,(M)\cap S_A$.

PROOF. We will construct an increasing sequence of countable sets $\langle A_n\colon n<\omega_0\rangle$, $A_n\subset A_{n+1}$ for $n<\omega_0$ and we will take $A=\bigcup\{A_n\colon n<\omega_0\}$. In order to construct M, in each step $n<\omega_0$ we will build monoids $M_{n+1}\subset {}^{A_{n+1}}(A_{n+1})$ by extending the elements of M_n to A_{n+1} and adding some (countable many) elements from ${}^{A_{n+1}}(A_{n+1})$. More precisely we construct the free $\circ$—generators of M_{n+1}. Finally every element of M_n will be extended to A for every $n<\omega_0$ and at the end we will take the set of generators of M to be the set of these extended functions.

(In terms of formulas, the set of generators of M is $F=\{\psi_{i,j}\colon i,\ j<\omega_0\}\subset {}^A A$ which we intend to define, $\psi_{i,n}$ "appears first" when constructing M_n (see below for definition). In step $n<\omega_0$ we will define the elements of the set $F_n=\{\psi_{i,j}\restriction A_n\colon i<\omega_0,\ j\leqq n\}\subset {}^{A_n}(A_n)$ only. This is the set of the generators of $M_n\subset {}^{A_n}(A_n)$. Since in the n^{th} step we have not constructed $\psi_{i,j}$ but $\psi_{i,j}\restriction A_n$ only, we write $\psi_{i,j}^{(n)}$ instead of $\psi_{i,j}\restriction A_n$ and define after the construction $\psi_{i,j}:=\bigcup\{\psi_{i,j}^{(n)}\colon n\geqq j\}$. For convenience we enumerate F_n as $\{\varphi_u^{(n)}\colon u<\omega_0\}$.)

From algebraic point of view, if M^* and M_n^* are the abstract monoids represented by M and M_n $(n<\omega_0)$, then M_n^* is a homomorph image of a submonoid of M_{n+1}^* for all $n<\omega_0$ and so M^* is the inverse limit of the system $\{\langle M_n^*, \vartheta_n\rangle\colon n<\omega_0\}$ where ϑ_n is the homomorphism mentioned above. Since every element of M map hierarchically (that is Range $(f\restriction(A_{n+1}\setminus A_n))\subset A_{n+1}\setminus A_n$ for every $f\in M$ and $n<\omega_0$ if f appeared before n) and is one-to-one; further the sets D, D_m for $m<v$, and v are finite in the definition of the local invertibility and the fairly completeness, these things are handled in A_m, and so in M_m for some $m<\omega_0$ large enough. Further, we construct the free generators of M_n and M only, so we can manage (i) through (iii) easily.

Now, let us get down into the details. Let A_0 be an arbitrary countable set, $F_0\subset {}^{A_0}(A_0)$ an arbitrary countable set of $\circ$—independent injective functions on it, and put $M_0:=\langle F_0, \circ\rangle$.

Suppose that we have already constructed A_n and M_n and now we want to construct A_{n+1} and M_{n+1}. We have $M_m=\langle F_m, \circ\rangle$ by construction, where $F_m=\{\psi_{i,j}^{(m)}\colon i<\omega_0,\ j\leqq m\}$ for all $m\leqq n$, and $\psi_{i,j}^{(k)}=\psi_{i,j}^{(m)}\restriction A_k$ for $i<\omega_0$, $j\leqq k\leqq m\leqq n$.

We want to extend the elements of F_n to A_{n+1} and find infinitely many local inverses for them on A_{n+1} as independent from each other as possible. To this end choose countable sets $B_{\psi,D,u}^{(n)}$ and $B_\psi^{(n)}$ disjoint from each other and from A_n for $\psi\in F_n$, $D\subset A_n$ finite, $u<\omega_0$ and, let P_{n+1} be not element of any of these sets and put

$$A_{n+1}:=A_n\cup\bigcup\{B_\psi^{(n)}\cup B_{\psi,D,u}^{(n)}\colon \psi\in F_n,\quad D\subset A_n\quad \text{finite},\quad u<\omega_0\}\cup\{P_{n+1}\}.$$

P_{n+1} ensures (iii); for further details see Lemma 1.3. $A_n\cup B_\psi^{(n)}$ will be the Range os $\psi\in F_n$ after extending it to A_{n+1} and $A_n\cup B_{\psi,D,u}^{(n)}$ will be the Range of a new element of F_{n+1}, the uth local inverse of $\psi\restriction D$ where $\psi\in F_n$ and $D\subset A_n$ is finite, $u<\omega_0$. The disjointness of the sets $B_\psi^{(n)}$ and $B_{\psi,D,u}^{(n)}$ is the main trick in the construction which ensures (i) through (iii). To be more precise, first extend all $\psi\in F_n$ to A_{n+1} to be one-to-one arbitrarily such that $\psi''(A_{n+1}\setminus A_n)\subset B_\psi^{(n)}$ and let $\{\psi_{i,j}^{(n+1)}\colon i<\omega_0,\ j\leqq n\}$ enumerate the set of these extended functions so that $\psi_{i,j}^{(n+1)}\restriction A_n=\psi_{i,j}^{(n)}$. (Recall that every $\psi\in F_n$ has the form $\psi_{i,j}^{(n)}$ for some $i<\omega_0$, $j\leqq n$.) Next let $l_{\psi,D,u}$ be the following injective function from A_{n+1} to $A_n\cup B_{\psi,D,u}^{(n)}$ for $\psi\in F_n$, $D\subset A_n$ finite for $u<\omega_0$: $l_{\psi,D,u}\restriction X=(\psi\restriction D)^{-1}$ and $l_{\psi,D,u}''(A_{n+1}\setminus X)\subset B_{\psi,D,u}^{(n)}$ where $X=\psi''D$. Finally put

$$\{\psi_{i,n+1}^{(n+1)}\colon i<\omega_0\}=\{l_{\psi,D,u}\colon \psi\in F_n,\ D\subset A_n \text{ is finite},\ u<\omega_0\}.$$

It is easy to see that all the functions $\psi_{i,j}^{(n+1)}$ for $i<\omega_0$, $j\leqq n+1$ are $\circ$— and -1—independent by the disjointness of the sets $B_\psi^{(n)}$, $B_{\psi,D,u}^{(n)}$, A_n for $\psi\in F_n$, $D\subset A_n$ finite, $u<\omega_0$. So we can define F_{n+1}, the set of generators of M_{n+1} as $F_{n+1}=$

$=\{\psi_{i,j}^{(n+1)}: i<\omega_0,\ j\leqq n+1\}$. Finally put $M=\langle F, \circ\rangle$ and $F=\bigcup\{\psi_{i,j}: i, j<\omega_0\}$ where $\psi_{i,j}=\bigcup\{\psi_{i,j}^{(n)}: n\geqq j\}$ for $i,j<\omega_0$. So we can say that the function $\psi=\psi_{i,j}\in F$ (or $\psi_{i,j}^{(j)}=\psi_{i,j}\restriction A_j$) *appeared first* in M_j, or shortly, at j, for any $i, j<\omega_0$.

So we have constructed A and M. Now we have to show that they have properties (i) through (iii).

It is easy to see that the elements of F are independent, so (i) holds.

Now we prove (iii). (Recall that F is enumerated as $\{f_i: i<\omega_0\cup\}$.)

LEMMA 1.3. *There is no permutation except* id_A *in* $\mathrm{Loc}(\langle H, \circ, -1\rangle)$ *for any* $H\subset F$ *finite.*

PROOF. We are given an $H\subset F$ finite and we must show that $\mathrm{Loc}(\langle H, \circ, -1\rangle)$ contains no permutation except id_A.

First choose an $n<\omega_0$ large enough such that all the members of H appeared first far below n (e.g. if $h\in H$ appeared first in M_{n_h}, $n_h<\omega$, then $n>n_h+1$ for $h\in H$.)

Suppose now $\pi\in\mathrm{Loc}(\langle H, \circ, -1\rangle)\cap S_A\setminus\{\mathrm{id}_A\}$. Let $a\in A$ be such that $\pi(a)\neq a$ and $D=\{P_{n+1}, \pi^{-1}(P_{n+1}), a\}$. Then we have

$$\pi\restriction D = (\varphi_k^{\varepsilon_k}\circ\varphi_{k-1}^{\varepsilon_{k-1}}\circ\ldots\circ\varphi_1^{\varepsilon_1}\circ\varphi_0^{\varepsilon_0})\restriction D$$

for some $k<\omega_0$, $\varphi_i\in H$ and $\varepsilon_i\in\{+1, -1\}$ for $i\leqq k$.

Using the facts that $\mathrm{Range}\,(\psi\restriction(A_{n+1}\setminus A_n))\subset B_\psi^{(n)}$ and $P_{n+1}\notin B_\psi^{(n)}$ for every $\psi\in F$ appeared first before n, clearly $\varepsilon_0=+1$ and since the sets $B_\psi^{(n)}$ for $\psi\in F$ are pairwise disjoint we can see (by induction on i) that $\varepsilon_i\neq\varepsilon_{i+1}$ implies $\varphi_i=\varphi_{i+1}$. Since $\pi(a)\neq a$ we can suppose that $\varepsilon_i=1-\varepsilon_{i+1}$ and $\varphi_i=\varphi_{i+1}$ holds for no $i\leqq k$. This means that $\varepsilon_i=+1$ for all $i\leqq k$. Finally $P_{n+1}\notin\mathrm{Range}\,(\varphi)$ for all $\varphi\in H$ but $P_{n+1}\in\in\pi''D$ shows a contradiction. □

So Lemma 1.2 (iii) holds.

Now we prove (ii).

LEMMA 1.4. *F is strongly fairly complete.*

Let us be given $\nu<\omega_0$, D_m, $\mathscr{H}_m$, g_m for $m<\nu$ and $f\in F$, $D\subset A$ finite as in Definition 1.1. We have to find some $t\in F$ with good properties.

Choose an $n<\omega_0$ large enough so that all these things appeared below n. That is we require that $\hat{D}\subset A_n$ where

$$\hat{D}:=D\cup f''D\cup\bigcup\{D_m\cup\mathrm{Range}\,(g_m):\ m<\nu\}$$

and every element ψ of $\hat{H}:=\{f\}\cup\bigcup\{\mathscr{H}_m: m<\nu\}$ appeared first below n. Write $\bar{f}$ for $f\restriction A_n$, so $\bar{f}\in F_n$.

When we built F_{n+1} we defined some local inverses $\bar{t}=l_{\bar{f},D,u}\in F_{n+1}$ $(u<\omega_0)$ for the present f and D and this $\bar{t}$ appears in the sequence $\{f_i\restriction A_{n+1}: i<\omega_0\}=F_{n+1}$ infinitely many times.

We now show that the functions $t\in F$ for which $t\restriction A_{n+1}=\bar{t}$ works. So, fix such a $t\in F$ and let $u<\omega_0$ its index.

We may work in M_{n+1} and A_{n+1} since $\psi''(A_{m+1}\setminus A_m)\subset A_{m+1}\setminus A_m$ for every. $\psi\in\hat{H}$ and $m>n$ since the elements of $\hat{H}$ appeared first at last $n+1$ and $\hat{H}\subset A_n$. (That is, all the functions we use from now on, we can suppose are elements of M_{n+1}, their Dom is A_{n+1}.) Let $m<\nu$ be fixed. Roughly speaking our construction works because we defined the values of our functions as independently as it was possible, that is ($\bar{f}$ stands for $f\restriction A_n$, $\bar{f}\in F$):

$$(!)\quad \mathrm{Range}\,(t\restriction(A_n\setminus f''D)) \subset B^{(n)}_{\bar{f},D,u} \quad \text{but} \quad \mathrm{Range}\,(f\restriction A_n) \subset A_n$$

$$(!!)\quad \mathrm{Range}\,(\varphi\restriction B^{(n)}_{\bar{f},D,u}) \subset A_{n+1}\setminus A_n \quad \text{for} \quad \varphi\in M \quad \text{appeared before } n$$

$$(!!!)\quad B^{(n)}_{\bar{f},D,u}\cap A_n = \emptyset \quad \text{and} \quad D\subset A_n.$$

Now we verify in details. We have to verify: if $g_m\neq \mathrm{id}\restriction D_m$ and $g_m\neq\varphi\restriction D_m$ for all $\varphi\in\langle\mathscr{H}_m, \circ, -1\rangle$ then for all $\varphi\in\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$ we have $\varphi\restriction D_m\neq g_m$. Namely we prove the following:

STATEMENT 1.5. *For arbitrary* $\psi\in\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$
(a) *EITHER t can be replaced by $(f\restriction D)^{-1}$ and t^{-1} by $f\restriction D$ in ψ everywhere and for the resulted ψ' we have $D_m\subset\mathrm{Dom}\,(\psi')$ and $\psi'\restriction D_m=\psi\restriction D_m$,*
(b) *OR* $\mathrm{Range}\,(\psi)\cap(A_{n+1}\setminus A_n)=\emptyset$.

This statement clearly implies that F is strongly fairly complete.

PROOF. Let $\psi\in\langle\mathscr{H}_m\cup\{t\}, \circ, -1\rangle$ be fixed. We can write ψ in the form

$$\psi = y_h^{\varepsilon_h}\circ y_{h-1}^{\varepsilon_{h-1}}\circ\ldots\circ y_2^{\varepsilon_2}\circ y_1^{\varepsilon_1}\circ y_0^{\varepsilon_0} \tag{1}$$

where $y_i\in\mathscr{H}_m\cup\{t\}$ and $\varepsilon_i\in\{+1, -1\}$ for $i\leqq h$ for some $h<\omega_0$.

Our goal is to replace t by $(f\restriction D)^{-1}$ in ψ as required in (a) whenever it is possible. We try to replace t in each of its occurrence in ψ separately step by step. (We are allowed to make a replacement if for the resulted $\tilde{\psi}$ we have $D_m\subset\mathrm{Dom}\,(\tilde{\psi})$.) If we succeed to replace all the occurrences of t by $(f\restriction D)^{-1}$ (and t^{-1} by $f\restriction D$) then we reach case (a). If not, we get a breakdown somewhere, we reach case (b).

Now we examine not only the structure of ψ but the "route" of D_m. That is, if $\psi_{i_0}''D_m$ once pops into $A_{n+1}\setminus A_n$ (ψ_{i_0} is an initial segment of ψ) then, by our construction, it does for all $i>i_0$, so finally ψ satisfies case (b). In the remainder part of the proof we verify the above in details. Now let the sequence $\langle i_r\colon r<w\rangle$ enumerate the indices $i\leqq h$ in increasing order for which $y_i=t$. We can clearly suppose that $w\neq 0$.

Case I: $\varepsilon_i=+1$ for all $i<h$. (In this case $\psi\in\langle\mathscr{H}_m\cup\{t\}, \circ\rangle$.) Now define $\psi_0=\psi_0'=\psi_0^{(0)}=\mathrm{id}$ and for $r<w$, $r>0$ put

$$\psi_r^{(0)} = y_{i_r-1}\circ y_{i_r-2}\circ\ldots\circ y_j\circ\psi_{r-1}$$
$$\psi_r = t\circ\psi_r^{(0)}$$
$$\psi_r' = (f\restriction D)^{-1}\circ y_{i_r-1}\circ\ldots\circ y_j\circ\psi_{r-1}'$$

where $j=i_{r-1}+1$.

(ψ_r and ψ_r' are the initial parts of ψ and ψ' resp., showing the procedure of replacing each occurrence of t by $(f\restriction D)^{-1}$ in ψ.)

Now our task is to prove by induction on $r<w$ that

$$(2)\quad \begin{cases} \text{(a)} \quad \text{EITHER} \quad D_m\subset\mathrm{Dom}\,(\psi_r') \quad \text{and} \quad \psi_r' D_m\restriction = \psi_r\restriction D_m \\ \text{(b)} \quad \text{OR} \qquad \mathrm{Range}\,(\psi_r\restriction D_m)\cap(A_{n+1}\setminus A_n)\neq\emptyset. \end{cases}$$

Obviously (2) for all $r<w$ implies that we are done. To see this observe that $\psi=y_h\circ\ldots\circ y_j\circ\psi_{w-1}$ and $\psi'=y_h\circ\ldots\circ y_j\circ\psi'_{w-1}$ where $j=i_{w-1}+1$.

Then (2) (a) for $r=w-1$ implies $D_m\subset\mathrm{Dom}(\psi')$ and $\psi'\restriction D_m=\psi\restriction D_m$ while (2) (b) for $r=w-1$ implies Range $(\psi_r\restriction D_m)\cap(A_{n+1}\setminus A_n)\neq\emptyset$ as required for Statement 1.5.

So, the induction step for (2): If case (b) holds in (2) for some $r_0<w$ then it is easy to see that for every $r>r_0$ case (b) holds in (2). So w.l.o.g. case (a) holds for every $r<w$. In this case, if we denote $(\psi_r^{(0)})''D_m$ by x, we have two subcases depending on the position of x:

Subacase (i): $x\subset f''D$. Then t can obviously be replaced by $(f\restriction D^{-1})$ in ψ_r and $\psi'_r\restriction D_m=\psi_r\restriction D_m$.

Subcase (ii): $x\nsubseteq f''D$. Then it is easy to see that t can not be replaced by $(f\restriction D)^{-1}$ since $t''(x\setminus f''D)\subset B^n_{f,D,u}\subset A_{n+1}\setminus A_n$ and so $D_m\nsubseteq\mathrm{Dom}(\psi'_r)$. So Range $(\psi'_r\restriction D_m)\cap(A_{n+1}\setminus A_n)\neq\emptyset$ which proves the induction step for r and so we proved Case I, too.

Case II: $\varepsilon_i=-1$ for some $i<h$. The method for this case is similar to the previous one but we have to be more careful.

Obviously we may suppose that there is no part like $y\circ y^{-1}$ in (1), i.e.

(3) for no $i<h$ we have $y_{i+1}=y_i$ and $\varepsilon_{i+1}=1-\varepsilon_i$

(since $g_m\neq\mathrm{id}\restriction D_m$). Again we examine the route of D_m. Put now $Y_{-1}=D_m$ and $Y_i=(y_i^{\varepsilon_i})''Y_{i-1}$ for $i\leqq h$. Let further e_0 be the smallest $e\leqq h$ such that $Y_i\cap(A_{n+1}\setminus A_n)\neq\emptyset$ if such an e does exist. Again we have two subcases:

Subcase (i): e_0 does exist. Then we know that for every $\varphi\in M_n$ we have Range $(\varphi^{+1})\subset A_n$ and Range $(\varphi^{-1})\subset A_n$. But e_0 was minimal and $D_m\subset A_n$ and $\hat{H}\subset M_n$, so we must have $e_0=i_{r_0}$ for some $r_0<w$. (The sequence $\langle i_r\colon r<w\rangle$ was defined before Case I.) In other words $y_{e_0}=t$. Further, by the construction of t and by the minimality of e_0 we have $\varepsilon_{e_0}=+1$ and $Y_{e_0}\cap(A_{n+1}\setminus A_n)\subset B^{(n)}_{f,D,u}$.

We know that for every $\varphi\in F_n$, $D\subset A_n$ finite and $i<\omega_0$ all the sets $B^{(n)}_\varphi$ and $B^{(n)}_{\varphi,D,u}$ are all pairwise disjoint, and for every $\varphi\in M_n$ we have Range $(\varphi\restriction(A_{n+1}\setminus A_n))\subset B^{(n)}_\varphi$.

So, by (3) we can prove by induction on i, $e_0\leqq i\leqq h$ the following fact (as in Lemma 1.3), using $\hat{H}\subset M_n$: $e_i=+1$ and there is a $\varphi=\varphi(i)\in F_n$ such that $Y_i\cap\cap(A_{n+1}\setminus A_n)\subset B^{(n)}_\varphi$ or $Y_i\cap(A_{n+1}\setminus A_n)\subset B^n_{\varphi,D,u}$. (This means that $\psi''D_m\cap\cap(A_{m+1}\setminus A_m)\neq\emptyset$.) This proves Subcase (i).

Subcase (ii): e_0 does not exist. Then for $i\leqq h$ we have $Y_i\subset A_n$. Now define ψ_r, $\psi_r^{(0)}$ and ψ'_r and prove (2) by induction on $r<w$ exactly on the same way as in Case I.

The induction step in case ("t^{ε_i} can be replaced by $(f\restriction D)^{1-\varepsilon_i}$ in ψ_r for every $r<w$") is as follows:

Let $x=(\psi_r^{(0)})''D_m$ and $\varepsilon=\varepsilon_{i_r}$. If $x\subset D$ and $\varepsilon=+1$ or $x\subset f''D$ and $\varepsilon=-1$ then clearly we can replace t^ε by $(f\restriction D)^{1-\varepsilon}$ in ψ_r and $\psi'_r\restriction D_m=\psi_r\restriction D_m$. In any other case we would have $Y_{i_n}=(t^\varepsilon)''x\subset A_n$ by the definition of t, which is impossible.

So we proved Lemma 1.4. □

So (ii) also holds in Lemma 1.2 and we concluded the proof of Lemma 1.2. □

2. Proof of the main theorem

In this section we prove:

THEOREM 2.1. CH *implies* $\neg P(2^{\aleph_0})$.

PROOF. Our task is to define a monoid $N \subset {}^B B$ on some set B such that $\mathrm{Loc}(N) \cap S_B = \{\mathrm{id}_B\}$. We start with the monoid $M \subset {}^A A$ constructed in the previous section. Then, using the main ideas of the previous section to extend the generators to larger and larger sets as independently as possible, step by step we extend M to B, killing the elements of $\mathrm{Loc}(M) \cap S_A \setminus \{\mathrm{id}_B\}$. We do not add any new generator, we only extend the elements of F (= the set of free generators of $M \subset {}^A A$) to B. Finally we will get N as the generatum of these extended generators.

So, let A, F and M be guaranteed by Lemma 1.2 and let $\{\pi_i : i < \omega_1\}$ enumerate $\mathrm{Loc}(M) \cap S_A \setminus \{\mathrm{id}_A\}$. In each step $j < \omega_1$ we extend A and the elements of F to a larger set B_{j+1} ($B_j \supset \bigcup\{B_u : u < j\}$ for all $j < \omega_1$, $B_1 = A$, $B_0 = \emptyset$) in such a way that π_i does not extend to B_{j+1} for some $j \geqq i$. (This means that for no $\varrho \in \mathrm{Loc}(M_{j+1})$ $\varrho \restriction A = \pi_i$ where $M_{j+1} \subset {}^{B_{j+1}}(B_{j+1})$ is the extended monoid.) In this case we say that we "killed π_i".

To be somewhat more precise, let A_i be arbitrary countable infinite sets disjoint from each other for $i < \omega_1$ and $A_0 = A$. Put $B_j = \bigcup\{A_i : i < j\}$ for $j \leqq \omega_1$ and $B = B_{\omega_1}$. (So $B_0 = \emptyset$ and $B_1 = A$.) Fix further a booking function δ mapping $\omega_1 \setminus \{0, 1\}$ onto $\omega_1 \times \omega_1$ with the property: $h \leqq j$ if $\delta(j) = (h, k)$ for some $j < \omega_1$ and for all $j, h < \omega_1$. (In the j^{th} step we will kill the $\delta(i) = (h, k)^{\text{th}}$ permutation, that is the k^{th} permutation of $\mathrm{Loc}(M_h) \subset {}^{(B_h)}B_h$ (the h^{th} level). We are forced to use such a booking function since $\varrho \restriction A = \mathrm{id}_A$ for many $\varrho \in \mathrm{Loc}(M_h) \setminus \{\mathrm{id}_{B_h}\}$, $h < \omega_1$ and finally we want to kill every elements of $\mathrm{Loc}(N) \setminus \{\mathrm{id}_B\}$ and $A \subset B_h \subset B$.)

Step by step we will extend (the generators of) M to B as follows. Let $M_1 = M$. Denote M_j the monoid already extended to B_j (so $M_j \subset {}^{B_j}B_j$ and $M_0 = B_0 = \emptyset$, $M_{\omega_1} = N \subseteqq {}^B B$) for $j \leqq \omega_1$. The set of generators of M_j for $j \leqq \omega_1$, $j \neq \emptyset$ is $F_j = \{f_k^{(j)} : k < \omega_0\} \subset {}^{(B_j)}B_j$ and they have the property $f_k^{(t)} = f_k^{(j)} \restriction B_t$ for $k < \omega_0$ and $0 < t < j \leqq \omega_1$ by the construction.

Let further $\{\pi_{j,k} : k < \omega_1\}$ enumerate $\mathrm{Loc}(M_j) \cap S_{B_j} \setminus \{\mathrm{id}_{B_j}\}$ for $j < \omega_1$. Now let i be given, $2 \leqq i < \omega_1$ and suppose that we have already constructed M_j for all $j < i$. Now we want to construct M_i. (Recall that $M_j = \langle F_{j,0} \rangle$ for $j < i$ and the elements of F_{j_1} extend the elements of F_{j_2} for $j_1 < j_2 < i$.)

In case i is limit we clearly take

$$f_k^{(i)} = \bigcup\{f_k^{(j)} : j < i\} \quad \text{for} \quad k < \omega_0;$$

and

$$F_i = \{f_k^{(i)} : k < \omega_0\}, \quad M_i = \langle F_{i,0} \rangle \subset (B_j)B_i.$$

If $i = j+1$ then we extend the $\circ$—generators of M_j to B_i ($= B_{j+1} = B_j \cup A$) in such a way that the resulted M_i will have the properties (i) through (iii) of Lemma 1.2 and $\pi_{\delta(j)}$ will have been killed. The latter means that there will be no permutation $\varrho \in S_{B_i}$ in $\mathrm{Loc}(M_i)$ such that $\varrho \restriction B_h = \pi_{\delta(j)}$, where $\delta(j) = (h, k)$ for some $k < \omega_1$ (since $\pi_{\delta(j)}$ is the k^{th} element of $\mathrm{Loc}(M_h) \cap S_{B_h} \setminus \{\mathrm{id} \restriction B_h\}$, $k < \omega_1$, $h \leqq j$).

This construction ensures that finally we will have a locally invertible (and, moreover, a still strongly fairly complete) monoid N ($= M_{\omega_1}$) on B ($= B_{\omega_1}$) such that $\mathrm{Loc}(N)\cap S_B=\{\mathrm{id}\}$. (To see this use the fact that every element of N maps $A_n=B_{n+1}\setminus B_n$ into A_n for every $n<\omega_1$ and so does every element of $\mathrm{Loc}(N)\cap S_B$. If then $\pi\in\mathrm{Loc}(N)\cap S_B$, $\pi\neq\mathrm{id}_B$, then $\pi\restriction B_h\neq\mathrm{id}\restriction B_h$ for some $h\in\omega_1$, and so, by the construction, $\pi\restriction B_h\in\mathrm{Loc}(M_h)\cap S_{B_h}\setminus\{\mathrm{id}_{B_h}\}$ say $\pi\restriction B_h=\pi_{h,k}$ for some $k<\omega_1$. Then $\delta(j)=(h,k)$ for some $j<\omega_1$, $j\geqq h$. In the j^{th} step, defining the elements of N on $A_j=B_{j+1}\setminus B_j$ we killed $\pi_{h,k}$, so $\varrho\restriction B_h\neq\pi_{h,k}=\pi\restriction B_h$ for each $\varrho\in\mathrm{Loc}(N_j)\cap\cap S_{B_j}$ which so holds for each $\varrho\in\mathrm{Loc}(N)\cap S_B$, a contradiction.)

Now we present a construction for $M_2=\langle F_2,\circ\rangle$, the other successor steps $i=j+1$ are the same. Write for convenience π and A_π instead of $\pi_{\delta(1)}$ and A_1. (Recall that $B_1=A_0=A$, $B_2=A\cup A_\pi$ and $M_1=M\subset^{B_1}B_1$, $M=\langle F,\circ\rangle$.) Step by step we extend the elements of F to A_π in ω_0 steps (A_π and F are countable) and we take these extended functions into $F_2=\{f_k^{(2)}\colon k<\omega_0\}\subset^{B_2}B_2$. We intend to define the values of $f_k^{(2)}$, $k<\omega_0$ on A_π as independent as possible.

After the n^{th} step we will have extended the first $k^{(n)}$ many elements of F to a finite set $W^{(n)}\subset A_\pi$. (The only important thing is that we extended only finitely many elements of F. We choose the first $k^{(n)}$ elements of F for convenience only.) Further we will have fixed finite sets $E_i\subset A$ for every $i\leqq k^{(n)}$. These $E_i=E_i^\pi$ sets are the most important objects in our construction. We require that $E_i\supset E_j$ for $i>j$ and $\varphi\restriction E_i\neq\pi\restriction E_i$ for every $\varphi\in\langle\{f_j\colon j\leqq i\},\circ,-1\rangle$. This can be done by Lemma 1.2 (iii). The sets E_i play an important role in choosing locally inverses for the extended functions and taking care of the fairly completeness of F_2 (see Case 3). Furthermore, in Lemma 2.2 we prove that if $a\in A_\pi$ is fixed, $\hat{\pi}\restriction A=\pi$ for some $\hat{\pi}\in\mathrm{Loc}(M_2)\cap\cap S_{A\cup A_\pi}$ and $m<\omega_0$ is large enough then for all $\varphi\in\langle H,\circ,-1\rangle$ either $\varphi(a)\neq\hat{\pi}(a)$ or $\varphi\restriction E_m\neq\pi\restriction E_m$ where $H=\{f_k^{(2)}\colon i\leqq m\}$; moreover this property is preserved in all further steps, that is H can be any finite subset of $F^{(2)}$. This clearly justifies that π will be killed.

Denote the extended functions by $\hat{f}_i$, that is $\mathrm{Dom}(\hat{f}_i)=A\cup W^{(n)}$ and $\hat{f}_i\restriction A=f_i$ for $i\leqq k^{(n)}$. To summarize: after the n^{th} step ($n<\omega_0$) we will have $W^{(n)}\subset A_\pi$ finite, $k^{(n)}<\omega_0$ and $\{\hat{f}_i\colon i\leqq k^{(n)}\}$ where $\hat{f}_i$ extends f_i to $A\cup W^{(n)}$. ($\hat{f}_i$ depends upon n but we do not indicate this.) Finally let $A_\pi=\{a_j\colon j<\omega_0\}$ and let γ be a function from ω_0 onto the set

$$\omega_0\times[A_0]^{<\omega}\times[A_\pi]^{<\omega}\times\omega_0\times[[A]^{<\omega}]^{\omega}\times[[A_\pi]^{<\omega}]^{<\omega}\times[[F]^{<\omega}]^{<\omega}\times[A^*]^{<\omega}$$

and γ takes every value infinitely many times, where $A^*=\{g\restriction D\colon g\in{}^AA,\ D\in[A]^{<\omega}\}$ and $[X]^{<\omega}=\{Y\subset X\colon Y \text{ is finite}\}$ for any set X.

The role of γ is similar to that of δ: enumerates the requirements for M_2 to be locally invertible and fairly complete. The requirements listed by γ will be satisfied during the construction, in Case 3, $n=3l$.

Now let us see the construction itself.

In the 0^{th} step we do nothing: $W^{(0)}=\emptyset$ and no element of F is extended, $k^{(0)}=0$.

The $(n+1)^{\text{th}}$ step: let $W=W^{(n)}\subset A_\pi$ be the set constructed in the previous step and the function $f_0,f_1,\dots,f_k$ already extended be $\hat{f}_0,\hat{f}_1,\dots,\hat{f}_k$ with fixed sets $E_0,E_1,\dots,E_k$ where $k=k^{(n)}$. In ω_0 steps we have to define $\hat{f}(a)$ for all $f\in F$, $a\in A_\pi$", and infinitely many locally inverses of $\hat{f}\restriction D$ for all $f\in F$, $D\subset A\cup A_\pi$ finite. In each step $n<\omega_0$ we either define $\hat{f}(a)$ for a new $a\in A_\pi$ or for a new $f\in F$ or we define some local inverse of an $\hat{f}\restriction D$, and we have to make each type of steps cofinally many times. Enumerate first A_π and F as $A_\pi=\{a_j\colon j<\omega_0\}$ and $F=\{f_k\colon k<\omega_0\}$.

Since the order of the steps is unimportant, for easier understanding we work modulo 3 and distinguish three cases:

Case 1: $n=3l+1$ for some $l<\omega_0$. If $a_l\in W^{(n)}$ then we have nothing to do i. e. $W^{(n+1)}=W^{(n)}$, $k^{(n+1)}=k^{(n)}$. Otherwise extend $f_0, f_1, \ldots, f_k$ $(k=k^{(n+1)}=k^{(n)})$ to $W^{(n+1)}=W^{(n)}\cup\{a_l\}$ totally independently from each other and the points used before. That is, for $i\leqq k$ let $\hat{f}_i(a_l)$ be an arbitrary element of the set

$$A_\pi-W^{(n)}-\{a_l\}-\bigcup\{\text{Range}\,(\hat{f}_j)\colon j\leqq k\}-\{\hat{f}_j(a_l)\colon j<i\}.$$

Then we put $W^{(n+1)}=W^{(n)}\cup\{a_l\}$ and $k^{(n+1)}=k^{(n)}$.

Case 2: $n=3l+2$ for some $l<\omega_0$. If $k=k^{(n)}\geqq l$ then we have nothing to do. (I.e. $W^{(n+1)}=W^{(n)}$, $k^{(n+1)}=k^{(n)}$.) If not, then extend all the functions $f_{k+1}, f_{k+2}, \ldots, f_l$ step by step to $W=W^{(n)}$ independently from each other and the points used before. That is, if $W=\{a_u\colon u<w\}$ for some $w<\omega_0$ then let for $u<w$ and i, $k<i\leqq l$ $\hat{f}_i(a_u)$ be an arbitrary element of the set

$$A_\pi-W-\bigcup\{\text{Range}\,(\hat{f}_j)\colon j<i\}-\{\hat{f}_i(a_t)\colon t<u\}.$$

Further, for every i, $k<i\leqq l$ by Lemma 1.2 (iii) (and by the induction hypothesis, that is M_m satisfies Lemma (i) through (iii) for every $m\leqq\omega_1$) we know that there is no bijection in $\text{Loc}\,(\langle f_j\colon j\leqq i\}, \circ, -1\rangle)$ except id_A. So we can choose an $E_i\subset A$ for $k<i\leqq l$ be finite such that $E_i\supset E_j$ and $\pi\restriction E_i\neq\text{id}\restriction E_i$ for $j<i$ and $\varphi\restriction E_i\neq\pi\restriction E_i$ for every $\varphi\in\text{Loc}\,(\langle\{f_t\colon t\leqq i\}, \circ, -1\rangle)$ and $k\leqq j<i\leqq l$. So in this case we construct $W^{(n+1)}=W^{(n)}$, $k^{(n+1)}=l$, $\hat{f}_{k+1}, \hat{f}_{k+2}, \ldots, \hat{f}_l$ and $E_{k+1}, E_{k+2}, \ldots, E_l$, too, $(k=k^{(n)})$ while $\hat{f}_i$ and E_i for $i\leqq k$ remain unchanged.

Case 3: $n=3l$ for some $l<\omega_0$. Now we have to do something only if $\gamma(l)$ codes a requirement for F_2 to be fairly complete.

First we clarify when $\gamma(l)$ codes such a requirement. We have

$$\gamma(l)=(l_1, X, Y, m_l, S_1, S_2, \zeta, G\rangle$$

where l_1, $m_l<\omega_0$ and $S_i=\{T_m^{(i)}\colon m<\nu^{(i)}\}\subset[A_i]^{<\omega_0}$ for some $\nu^{(i)}<\omega_0$, $i=1,2$ recall that $A_1=A$, $A_2=A_\pi$) and

$$\zeta=\{\mathcal{H}_m\colon m\lneqq\nu^{(3)}\}\subset[F]^{<\omega_0}\quad\text{for some}\quad\nu^{(3)}<\omega_0$$

and

$$G=\{g_m\colon m\lneqq\nu^{(4)}\}\subset A^*\quad\text{for some}\quad\nu^{(4)}<\omega_0.$$

Then $\gamma(l)$ codes such a requirement iff $|G|=|S_1|=|S_2|=|\zeta|=\nu$ and for every $m<\nu$ $\text{Dom}\,(g_m)=T_m^{(1)}$.

If the above statement does not hold then we have nothing to do. If it does, then we will construct m_l many locally inverses of $\hat{f}_{l_1}(X\cup Y)$ with taking care of the fairly completeness of F_2 with respect to $\mathcal{H}_m$ and

$$\hat{D}_m:=T_m^{(1)}\cup T_m^{(2)}\quad(m<\nu).$$

Now do the following construction m_l times, repeatedly. (Repeatedly here means true physically repetitions: after one construction ends we start the whole procedure once more again from the very beginning, repeatedly increasing $k^{(n+1)}$ and $W^{(n+1)}$.)

First we have to suppose that $k=k^{(n)}$ and $W=W^{(n)}$ are large enough, that is $k\geqq l_1$, $k>\max\{t<\omega_0: f_t\in\mathscr{H}_m,\ m<v\}$ and $W\supset Y\cup\bigcup S_2\cup(\hat{f}_{l_1})''Y$. (If not, use the constructions described in Cases 1 and 2.)

In the construction we use the fairly completeness of F. We have already g_m, $\mathscr{H}_m$ for $m<v$. Now link the sequence $\pi\restriction E_i$ and $\{f_j: j\leqq i\}$ for $i\leqq k^{(n)}$ to the above sequence, that is put

$$g_{v+i}:=\pi\restriction E_i \quad\text{and}\quad \mathscr{H}_{v+i}:=\{f_j: j\leqq i\} \quad\text{for}\quad i\leqq k^{(n)},\quad\text{so}\quad v=v+k^{(n)}+1.$$

Further, write f_{l_1} and X instead of f and D in Definition 1.1. Since F is fairly complete we have a function $t\in F$ with good properties; moreover such that $t\notin\{f_i: i\leqq k^{(n)}\}$. t is good in A. We will extend it to $W^{(n)}$ taking care of $\hat{f}$, Y and $T_m^{(2)}$ and arbitrary functions $\hat{g}_m$ on $T_m^{(2)}$ for $m<v$. The sets $T_m^{(2)}$ for $m<v$ are settled since $\bigcup\{T_m^{(2)}: m<v\}\subset W^{(n)}$. The sets $T_m^{(2)}$ for $v\leqq m<v$ and the functions $\hat{g}_m$ on $T_m^{(2)}$ for $m<v$ are unimportant since we will define $\hat{t}$ on $W^{(n)}$ (and later on further sets) totally independently from the other functions.

Now use the construction described in Case 2 to extend the functions f_i for $k<i\leqq k(t)$ to $W^{(n)}$ and determine the sets E_i with the method described in Case 2 with the restriction $\hat{t}\restriction(\hat{f}''Y)=(\hat{f}\restriction Y)^{-1}$ where $k(t)$ is defined as $t=f_{k(t)}\in F$. Though $R(\hat{t})$ is not disjoint from $W^{(n+1)}=W^{(n)}$, we will see in the proof (see Lemmas 2.2 and 2.4) it does not make any trouble. Finally we put $W^{(n+1)}=W^{(n)}$ and $k^{(n+1)}=k(t)$ (and possibly repeat the construction m_l-1 times again). (To be somewhat more precise: let $W^{(n)}=\{a_u: u<w\}$ and for i, $k<i\leqq k(t)$ and $u<w$ if $i\neq k(t)$ or $a_u\notin f''Y$ then let $f_i(a_u)$ be an arbitrary element of the set

$$A_\pi\setminus W^{(n)}\cup\{\hat{f}_r W^{(n)}: r\leqq k\}\setminus\{\hat{f}_r(a_s): s\leqq u,\ r<i\}).$$

This ends the construction. □

So we have extended all the generators of M to A_π. Let the $\circ$—generators of M_2 be F_2, the set of these extended $\hat{f}_i$ functions, $i<\omega_0$. We have to show that M_2 satisfies the requirements (i) through (iii) in Lemma 1.2 and that π does not extend to A_π. (i) and (iii) can be easily verified.

We only have to check that F_2 is strongly fairly complete and that π does not extend to A_π. (The other requirements are clearly satisfied.)

Lemma 2.2. *π is not extended to A_π.*

Proof. We prove a bit more: π can not be extended to an element of $\mathrm{Loc}(\langle F_2,\circ,-1\rangle)\cap S_{A\cup A_\pi}$.

Suppose it does. Let $a\in A_\pi$ be arbitrary fixed. If there is a $\hat{\pi}\in\mathrm{Loc}(\langle F_2,\circ,-1\rangle)\cap\cap S_{A\cup A_\pi}$ such that $\hat{\pi}\restriction A=\pi$ then $b=\hat{\pi}(a)=(\hat{f}_{i_1}\circ\hat{f}_{i_2}\circ\ldots\circ\hat{f}_{i_s})(a)$ for some $i_0, i_1, \ldots, \ldots, i_s<\omega_0$ and $s<\omega_0$. By the construction there is an $n<\omega_0$ large enough such that we have already extended all the functions f_{i_j} $(j\leqq s)$ till the n^{th} step so that $(\hat{f}_{i_0}\circ\hat{f}_{i_1}\circ\ldots\circ\hat{f}_{i_s})(a)$ is meaningful and equals $b\in W^{(n)}$. (That is, $k^{(n)}\geqq i_j$ for $j\leqq s$ and $(\hat{f}_{i_t}\circ\ldots\circ\hat{f}_{i_s})(a)$ for $0<t\leqq s$ and b are elements of $W^{(n)}$.)

Now fix such an arbitrary $n<\omega_0$. Recall that till the n^{th} step we have extended f_i $(i\leqq k\leqq k^{(n)})$ to $W=W^{(n)}$ and fixed the sets $E_i\subset A$ $(i\leqq k)$. By the definition of the set E_k we have $\varphi\restriction E_k\neq\pi\restriction E_k=\hat{\pi}\restriction E_k$ for every $\varphi\in\langle\{f_i: i\leqq k\},\circ,-1\rangle$ and $\pi\restriction E_k\neq\mathrm{id}\restriction E_k$. But by our indirect assumption there is a $k'<\omega_0$ such that $\psi\restriction E_k=$

$=\hat{\pi}\restriction E_k=\pi\restriction E_k$ for some $\psi\in\mathrm{Loc}\langle\{f_j:\ j\leqq k'\},\circ\rangle$ since $\hat{\pi}\in\mathrm{Loc}(M_2)$. Clearly we have $k'>k$ and we must have extended the functions $f_k,\dots,f_{k'}$ till the n^{th} step, $n'>n$ and $k'=k^{(n')}$.

However the following result can be proved by induction on m, $m>n$, using that F_1 is fairly complete:

CLAIM 2.3. *For arbitrary* $m\geqq n$ *if we have extended the functions* f_i $(i\leqq k^{(n)})$ *to* $W^{(m)}$ *in steps* $0, 1, \dots, m$ *then for every* $\varphi\in\langle\{\hat{f}_i:\ i\leqq k^{(m)}\},\circ,-1\rangle$ *either* $\varphi(a)\neq b$ *or* $\varphi\restriction E_k\neq\pi\restriction E_k$ *(here* $k=k^{(n)}$ *and n is fixed.)*

Obviously this claim proves Lemma 2.2.

PROOF. The proof is an easy induction on m, examining the effect of the construction in all three cases. The heart of our construction is that we always extended the functions totally independently from everything (the other functions and the points used before with a small restriction in Case 3).

The proof is rather easy but technical. The claim for $m=n$ is valid. Let $m\geqq n$ and $k^{(m)}$, $W^{(m)}$ as usual. We prove for $m+1$.

Fix any $\varphi\in\langle\{\hat{f}_i:\ i\leqq k^{(m+1)}\},\circ,-1\rangle$, say

$$\varphi=\hat{y}_0^{\varepsilon_0}\circ\hat{y}_1^{\varepsilon_1}\circ\dots\circ\hat{y}_s^{\varepsilon_s}\quad(s<\omega_0,\ \varepsilon_n\in\{+1,-1\}\ \text{for}\ u\leqq s)\tag{4}$$

where $\hat{y}_u=\hat{f}_{i_u}$, $i_u\leqq k^{(m)}$. We have to show that either $\varphi(a)\neq b$ of $\varphi\restriction E_k\neq\pi\restriction E_k$ ($k=k^{(n)}$ is fixed), using that this statement holds for m, that is for all $\psi\in\langle\{\hat{f}_i:\ i\leqq k^{(m)}\},\circ,-1\rangle$. Suppose that $\varphi\restriction E_k=\pi\restriction E_k$ and $\varphi(a)=a$. Then we have $\varphi\restriction E_k\neq\mathrm{id}\restriction E_k$ since $\pi\restriction E_k\neq\mathrm{id}\restriction E_k$. So we may suppose that there is no part like $f\circ f^{-1}$ or $f^{-1}\circ f$ in φ. (That is in (4) there is no $u<s$ such that $y_u=y_{u+1}$ and $\varepsilon_u=1-\varepsilon_{u+1}$.)

According to the construction we have to distinguish three cases—which one was carried out to construct $k^{(m+1)}$, $W^{(m+1)}$, etc.

Case 1: $m=3l+1$ for some $l<\omega_0$. Then we extended the functions (among other functions) $\hat{y}_u$ $(u\leqq s)$ to $W^{(m+1)}=W^{(m)}\cup(a_l)$ totally independently from each other and the points used before. Since the induction hypothesis holds for m, by the construction it also holds for $m+1$.

Case 2: $m=3l+2$ for some $l<\omega_0$. Then $k^{(m+1)}\geqq l$ and we extended the functions $f_{k^{(m)}+1},\dots,f_l$ to $W^{(m+1)}=W^{(m)}$ totally independently from each other and the points used before. Since the induction hypothesis holds for m, it also holds for $m+1$, as well. (If $i_u>k^{(m)}$, that is there is a new function in (4), not constructed till the m^{th} step, we must have $\varphi(a)\neq b$. If not, then φ was constructed in the m^{th} step, and so we can use the induction hypothesis.)

Case 3: $m=3l$ for some $l<\omega_0$. This is the most crucial part of our proof.

In this case we constructed for some $l_1\leqq k^{(m)}$ (several) locally inverses $\hat{f}_t$ of the function $\hat{f}_{l_1}$ with respect to a set $X\cup Y\subset A\cup A_\pi$ $(l_1\leqq k^{(m)}<t\leqq k^{(m+1)},\ Y\subset W^{(m)})$. We took an $f_t\in F_1$, using the strongly fairly completeness of F_1, with respect to (among others) $\hat{\pi}\restriction E_k$ ($k=k^{(n)}$ is fixed) and extended f_t to $W^{(m+1)}=W^{(m)}$ totally independently from the functions and points used before (with the only restriction that $\hat{f}_t\circ\hat{f}_{l_1}\restriction Y=\mathrm{id}\restriction Y$ but this causes no trouble since $Y\cup(\hat{f}_{l_1})''Y\subset W^{(m)}$).

If $i_u\neq t$ for all $u<s$ (that is $\hat{f}_t$ does not appear in φ in (4)) then by (4) we know

that φ has already been constructed before the $(m+1)^{\text{th}}$ step and using the induction hypothesis we are done.

So $\hat{f}_t$ appears in (4).

Write φ' for the function we get by replacing $\hat{f}_t$ by $(\hat{f}_{l_1}\restriction(X\cup Y))^{-1}$ and $(\hat{f}^t)^{-1}$ by $\hat{f}_{l_1}\restriction(X\cup Y)$ in φ. Using the good properties of f_t by the strongly fairly completeness of F_1 and our indirect assumption $\varphi\restriction E_k=\pi\restriction E_k$ we may replace f_t by $(f_{l_1}\restriction X)^{-1}$ in $\varphi\restriction A$ everywhere and so we have $\varphi'\restriction E_n=\varphi\restriction E_k=\pi\restriction E_k$ ($k=k^{(n)}$ is fixed).

Next we show that we can derive $\varphi'(a)=b$ using the indirect assumption $\varphi(a)=b$. We defined $\hat{f}_t$ totally independently on $W^{(m)}\setminus\text{Range}(\hat{f}_l\restriction Y)$ from the points used before and we defined $\hat{f}_t$ on $\text{Range}(\hat{f}_{l_1}\restriction Y)$ to be the inverse of $\hat{f}_{l_1}\restriction Y$. It follows that supposing $\varphi(a)$ is meaningful and equals to b we have that $\varphi'(a)$ is meaningful and equals $\varphi(a)=b$ (since b was an old point, too, that is $a, b\in W^{(m)}$ and $Y\cup(\hat{f}_{l_1})''Y\subset W^{(m)}$).

So we have $\varphi'\restriction E_k=\pi\restriction E_k$ and $\varphi'(a)=\varphi(a)=b=\hat{\pi}(a)$. But φ' only consists of functions constructed before the $(m+1)^{\text{th}}$ step and by the induction hypothesis this is a contradiction.

So we proved Claim 2.3 and so Lemma 2.2. too. □

In order to carry out our construction in further steps (for M_3, M_4, ... and for any M_{i+1} $(i<\omega_1)$) we must also to preserve the strongly fairly completeness of F.

LEMMA 2.4. *F_2 is strongly fairly complete.*

PROOF. The proof is mainly included in the construction: in Case 3 we manage the fairly completeness of F_2, and do not destroy it in further steps.

Observe first that the following fact is true: for every $n_1<n_2<\omega_0$ if untill the n_i-th steps $(i=1, 2)$ we have extended the functions $\{f_j\colon j\leqq k^{(n_i)}\}$ to the functions $\{\hat{f}_j^{(i)}\colon j\leqq k^{(n_i)}\}$, $\text{Dom}(\hat{f}_j^{(i)})=A\cup W^{(n_i)}$ for $j\leqq k^{(n_i)}$ and $i=1, 2$ then we have

$$W^{(n_1)}\subseteqq W^{(n_2)} \quad\text{and}\quad \hat{f}_j^{(1)}\subseteqq\hat{f}_j^{(2)} \quad\text{for}\quad j\leqq k^{(1)} \tag{5}$$

$$\text{Range}(\hat{f}_i^{(1)}\restriction W^{(n_1)})\cap\text{Range}(\hat{f}_j^{(2)}\restriction(W^{(n_2)}\setminus W^{(n_1)}))=\emptyset \quad\text{for}\quad i, j<k^{(n_1)}. \tag{6}$$

(That is: (5) says that we keep extending our functions, and (6) says that we define all functions independently from each other and the points used before.)

This fact can be proved by a simple induction on n_2, $n_1\leqq n_2<\omega_0$.

Now, recall that $F_2=\{\hat{f}_i\colon i<\omega_0\}$, $\hat{f}_i\restriction A=f_i\in F_1$ for $i<\omega_0$. Let us be given $v<\omega_0$, $D\subset A\cup A_\pi$, $\hat{f}_j\in F_2$, $\mathscr{H}_m\subset F_2$, $D_m\subset A\cup A_\pi$ finite and $g_m\colon D_m\to A\cup A_\pi$ for $m<v$ as in the definition of strongly fairly completeness. We have to find some $t=t(j)<\omega_0$ such that $\hat{f}_t$ has certain good preperties.

Clearly we may suppose that

$$\text{Range}(g_m\restriction(A\cap D_m))\subset A \quad\text{and}\quad \text{Range}(g_m\restriction(A_\pi\cap D_m))\subset A_\pi$$

for $m<v$. Choose an $n_0<\omega_0$ large enough such that in the n_0-th step we can talk about the above functions and sets, that is we have already extended all the elements of the set

$$\hat{H}=\{f_j\}\cup\{f_u\colon \hat{f}_u\in\mathscr{H}_m,\ m<v\}$$

to the set $W^{(n_0)}\subset A_\pi$, and $\hat{D}\cap A_\pi\subset W^{(n_0)}$ where

$$\hat{D}=D\cup\bigcup\{D_m\cup\text{Range}(g_m)\colon m<v\}\cup f_j''D.$$

We know that there are infinitely many $l_0 > n_0$ large enough such that in the $n=3l_0$-th step we found a local inverse f_t of $\hat{f}_j \upharpoonright D$ with respect to g_m and $\mathscr{H}_m$ $(m<v)$ taking care of the fairly completeness of F_2. (See Case 3 of the construction.) By the construction we have exactly one $\hat{f}_t \in F_2$ such that $\hat{f}_t \upharpoonright A = f_t$. We claim that $\hat{f}_t$ works.

Roughly speaking, $\hat{f}_t$ was extended as independently from $W^{(n)}$, the points and the functions used before as possible and this causes $\hat{f}_t$ to work.

Obviously we have $\hat{f}_t \circ (\hat{f}_j \upharpoonright D) = \mathrm{id}$. We have no trouble with the sets $D \cap A$, $D_m \cap A$ and $g_m \upharpoonright (D_m \cap A)$ $(m<v)$ since all members of F_2 map A into A and A_π into A_π and F_1 was strongly fairly complete. We also do not have trouble with the sets $D \cap A_\pi$, $D_m \cap A_\pi$ and $g_m \upharpoonright (D_m \cap A_m)$ $(m<v)$ using the construction (that is $\hat{f}_t$ was defined totally independently) and (5) and (6) for induction for $m>n$. By the construction the set $\{\hat{f}_i^{(n)}: i \leqq k^{(n)}\}$ is strongly fairly complete for the full sets D, D_m, g_m and $\mathscr{H}_m$ $(m<v)$. Further (5) and (6) ensure that we can not damage these good properties of $\hat{f}_t$ in any further step $m<\omega_0$ for $m>n$.

Finally, since this holds for all $m<\omega_0$ (m is large enough), it must hold for F_2 also (better to say, for $\hat{f}_t \in F_2$).

This proves Lemma 2.4 and so Theorem 2.1. □

3. Further results

In this section we use the ideas of Sections 1 and 2 to prove further theorems.

THEOREM 3.1. (a) MA *implies* $\neg P(2^{\aleph_0})$.

(b) MA(λ) *implies* $P(\lambda)$ *for* $\lambda < 2^{\aleph_0}$ *and for countable monoids.*

PROOF. (a) The method is rather similar to the one presented in the proof of Theorem 2.1. Let $\{\pi_i: i<2^{\aleph_0}\}$ enumerate $\mathrm{Loc}(M) \cap S_A - \{\mathrm{id}_A\}$, let A_j be pairwise disjoint countable sets for $j<2^{\aleph_0}$, $A_0 = A$ and let $B_i = \bigcup \{A_j: j<i\}$ for $i \leqq 2^{\aleph_0}$. Extend the elements of M succesively to B_i by killing π_i (and of course use the coding function $\delta: 2^{\aleph_0} \to 2^{\aleph_0} \times 2^{\aleph_0}$ as in Theorem 2.1 and use the fact that MA implies $2^\tau = 2^{\aleph_0}$ for $\tau < 2^{\aleph_0}$). The only difference is the succesive step: killing a permutation $\pi \in \mathrm{Loc}(M) \cap S_A$.

First we briefly sketch how to find a suitable forcing notion $\langle P, \leqq \rangle$ in the proof of Theorem 2.1. We know that the set of generators of M is $F = \{f_i\ i<\omega_0\}$ and there is no permutation in $\mathrm{Loc}(\langle \{f_j: j<i\}, \circ, -1 \rangle)$ for every $i<\omega_0$. So for every $i<\omega_0$ we can fix a finite subset $E_i \subset A$ such that $\varphi \upharpoonright E_i \neq \pi \upharpoonright E_i$ for every $\varphi \in \mathrm{Loc}(\langle \{f_j: j<i\}, 0, -1 \rangle)$ and $E_i \subset E_j$ for $i<j<\omega_0$, Let $\langle P^{(0)}, \leqq^{(0)} \rangle$ be the following forcing notion: $P^{(0)}$ consists of the forcing conditions of the form

$$p = \langle D^{(p)}, \langle \hat{f}_1^{(p)}, \ldots, \hat{f}_{k^{(p)}}^{(p)} \rangle \rangle$$

such that $k^{(p)} < \omega_0$, $D^{(p)}$ is a finite subset of A_π and $\hat{f}_i^{(p)}$ is a one-to-one extension of f_i to $A \cup D$ for $i \leqq k^{(p)}$.

Define the partial order $\leqq^{(0)}$ on $P^{(0)}$ as $p_1 \leqq^{(0)} p_2$ iff $k^{(2)} \leqq k^{(1)}$ and for every $i \leqq k^{(p_2)}$ $\hat{f}_i^{(p_2)} \subseteq \hat{f}_i^{(p_1)}$. Now define the subordering $\leqq$ of $\leqq^{(0)}$ as $p_1 \leqq p_2$ iff we obtained p_1 from p_2 using some (but finite) steps described in the proof of theorem 2.1. Clearly the largest element of P^0 is $1_P = \langle 0, 0 \rangle$. Then we define $\langle P, \leqq \rangle$ as $P = \{p \in P^{(0)}: p \leqq 1_P\}$ and we have already defined $\leqq$ above.

P is countable so it satisfies the ccc.

The following subsets of P are dense:

$$D_a = \{p \in P\colon a \in D^{(p)}\} \quad \text{for} \quad a \in A_\pi,$$

$$D_j = \{p \in P\colon j \leqq k^{(p)}\} \quad \text{for} \quad j \leqq \omega_0,$$

and

$$D_{j,m,D} = \{p \in P\colon j \leqq k^{(p)} \text{ and } D \cup \hat{f}_j'' D \subset D^{(p)}$$

and $\hat{f}_j \upharpoonright D$ has at least m locally inverse among the functions $\{\hat{f}_j\colon j \leqq k^{(p)}\}\}$ for $j, m < \omega_0$ and $D \subset A \cup A_\pi$ finite .

Applying Martin's axiom we get the desired extension of our monoid M to $A \cup A_\pi$ as in Theorem 2.1. □

(b) Let $|A| = \lambda$. The forcing notions

$$P_{f,D} = \{g \upharpoonright H;\ g \in M,\ H \in [A]^{<\omega},\ f \upharpoonright (H \cap D) = g \upharpoonright (H \cap D)\} \quad (f \in M,\ D \in [A]^{<\omega})$$

ordered by reversed inclusion satisfy the ccc since M is countable. By MA we get a generic subset $G \subset P$ intersecting all the dense sets $D_a = \{g \upharpoonright H \in P_{f,D}\colon a \in H \ \&\ a \in \text{Range}\,(g \upharpoonright H)\}$ for $a \in A$. This proves Theorem 3.1. □

THEOREM 3.2. *$2^{\aleph_0} = \aleph_2 + \neg\text{MA}$ with $\neg P(2^{\aleph_0})$ is consistent.*

PROOF. The forcing notion P defined in the proof of Theorem 3.1 is countable so we can apply a weak form of Martin's axiom which is consistent with $2^{\aleph_0} = \aleph_2 + \neg\text{MA}$:

THEOREM 3.3 (C. Hernik, [W, Theorem 5.7, p. 848]). *If there is a model of set theory then there is one in which we have*

(i) $2^{\aleph_0} = \aleph_2$,

(ii) SH,

(iii) MA($\aleph_0$-*linked*)

(iv) $\neg$ MA.

(For the definitions see e.g. [*K*] or [*W*].)

We only have to know that every countable poset is $\aleph_0$-linked. Then we proceed as in the proof of Theorem 3.1 (a) and apply Herink's theorem. Use the fact that MA($\aleph_0$-linked) also implies $2^\tau = 2^{\aleph_0}$ for $\tau < 2^{\aleph_0}$. This proves Theorem 3.2.

REMARK. We could get a suitable model for Theorem 3.2 simply adding $\aleph_2$ Cohen reals to an arbitrary model of ZFC (well-known or see e.g. [*W*]).

THEOREM 3.4. *$2^\lambda = \lambda^+$ implies $\neg P(2^\lambda)$ for any cardinal λ.*

PROOF. First construct a set C and a monoid $M_\lambda \subset {}^C C$ both of power λ taking λ disjoint copies of M constructed in Lemma 1.2. (In other words let $C = \cup\{C_i\colon i < \lambda\}$ where C_i are pairwise disjoint sets of power $\aleph_0$ and let $M_i \subset {}^{C_i}C_i$ be a monoid isomorphic to M of Lemma 1.2 with generator set F_i.) Put $\hat{F}_i = \{f \in {}^C C\colon f \upharpoonright C_i = f'$ and $f \upharpoonright (C - C_i) = \text{id}$ for some $f' \in F_i\}$ and let $F_\lambda = \cup\{\hat{F}_i\colon i < \lambda\}$ and $M_\lambda = \langle F_\lambda, 0\rangle$. Clearly F_λ satisfies the properties described in Lemma 1.2. Now extend M_λ step by step to a set of power of λ^+ by killing every permutation in Loc (M_λ) using a coding function δ: $\lambda \to \lambda \times \lambda$. When we kill a single permutation π we extend the elements of F_λ to $C \cup C_\pi$ where $|C_\pi| = \lambda$, in λ setps (where the sets C_π are pairwise disjoint). I do not think the details are worth writing down. $\square$

The same argument proves $\neg P(\varkappa)$ for $\varkappa$ strong limit.

References

[C] *Lectures in universal algebra*, ed. L. Szabó—Á. Szentenderi, Colloquia Math. Soc. J. Bolyai 43, North-Holland (Budapest, 1986).

[K] K. Kunen, *Set Theory — an introduction to independence proofs*, North-Holland, 1980.

[P1] R. Pöschel, Closure properties for relational systems with given endomorphism structure, *Beitrage zur Algebra und Geometrie*, Martin-Luther Universität, Halle-Wlittenberg, Heft **18** (1984), 153—166.

[P2] R. Pöschel,Concrete representation of algebraic structures and a general Galois theory, *Contributions to General Algebra*, Proc. Klagenfurt Conf. 1978, 249—272.

[P3] R. Pöschel, A general Galois theory for operations and relations and relations and concrete characterization of related algebraic structures, Report R—01/80, Zentralinstitut f. Math. u. Mech. (Berlin 1980), p. 101.

[PS] P. Prőhle—M. G. Stone, Extending monoid representations, *Contributions to General Algebra*, 3. Proc. Vienna conf. (June 1984).

[St] M. G. Stone, On endomorphism structure for algebras over a fixed set, *Coll. Math.*, **33** (1975), 41—45.

[Sz] I. Szalkai, On the algebraic structure of primitive recursive functions, *Zeitschrift f. Math. Logik u. Grundl. Math.*, **31** (1985), 551—556.

[W] W. Weiss, Versions of Martin's Axiom, in: *Handbook of Set-Theoretical Topology*, ed. K. Kunen and J. E. Vaughan, pp. 827—886.

(Received February 18, 1988; revised November 13, 1989)

DEPARTMENT OF MATHEMATICS
CHEMICAL UNIVERSITY
H—8201 VESZPRÉM, PF. 158.
HUNGARY