MAPPINGS OF SYMMETRIC SEMIGROUPS

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, and Computer Science Emeritus
Ohio State University
Columbus, Ohio 43210
https://u.osu.edu/friedman.8/
February 6, 2021

Abstract. The symmetric semigroups are the semigroups DD of all functions from the set D into D, under composition. (These are monoids in light of the identity map.) The surjective equation preserving mappings of DD and the automorphisms of DD are the same, and are exactly the mappings of DD induced by bijections of D by conjugation. (These must preserve the identity.) Every infinite DD has a non surjective equation preserving mapping into itself (and which preserves the identity element). We seek non surjective mappings of DD with stronger preservation. Most notably, does every infinite DD have a non surjective mapping preserving the solvability of finite sets of equations with parameters (solvable equation preserving)? (We show that any solvable equation preserving mapping must preserve the identity.) Even the existence of such DD is neither provable nor refutable from the usual ZFC axioms for mathematics, as such DD must be too large to fall within the grasp of ZFC (its cardinality must be far greater than a measurable cardinal). In fact, we show that the existence of such DD is equivalent to a very strong large cardinal hypothesis known as I2. I2 is far stronger than, say, the existence of a measurable cardinal. The existence of a non surjective mapping of some DD that preserves all first order statements (elementary embedding) is equivalent to the even stronger large cardinal hypothesis I1. We show that every mapping of every symmetric semigroup that is what we call absolutely preserving is surjective.

1. SEMIGROUP MAPPING BASICS

1.1. PRELIMINARIES

In these preliminaries, we consider mappings from one semigroup into another, even though the focus of the paper is entirely on mappings from one semigroup into itself. As this subject develops, we expect that mappings from one semigroup into a different one will play an important role.

Here we take a mapping of a semigroup to always be a mapping of the semigroup into itself.

DEFINITION 1.1.1. A semigroup is a pair G = (G,•), $\bullet G^2 \to G$, where • is associative. I.e., for all x,y,z ∈ G, (x•y)•z = x•(y•z). We omit • if it causes no confusion. I.e., (xy)z = x(yz). In a minor abuse of notation, j:G → H is a mapping from G into H where the • of G,H is not involved. j:G → H is a morphism if and only if for all x,y ∈ G, j(xy) = j(x)j(y). j:G → H is a monomorphism if and only if j is a morphism that is one-one. An isomorphism j:G → H is a surjective monomorphism. An automorphism of G is an isomorphism j:G → G.

In this paper, G,H always represents semigroups (G,•),{H,•). Symmetric semigroups (defined below) are certain special important semigroups, which are the focus of this research.

We can rethink morphisms and monomorphisms in terms of equation preserving mappings. In fact, the entire focus of this paper is on mappings with preservation properties.

DEFINITION 1.1.2. Let G be a semigroup. An equation is some $x_1...x_n = y_1...y_m$, $n,m \geq 1$, where $x_1,...,x_n,y_1,...,y_m \in G$. A basic equation is an equation where $n+m \leq 3$. $j:G \to H$ is (basic) equation preserving if and only if any given (basic) equation holds in G if and only if it holds in H when all of its terms are replaced by their values under j.

LEMMA 1.1.1. Let $j:G \to H$ be a morphism of G. Then $j(x_1...x_n) = j(x_1)...j(x_n)$.

Proof: By induction on $n \geq 2$. $n = 2$ is by the definition of morphism. $j(x_1...x_{n+1}) = j((x_1...x_n)x_{n+1}) = j(x_1...x_n)j(x_{n+1}) = j(x_1)...j(x_n)j(x_{n+1})$. QED

THEOREM 1.1.2. Let $f:G \to H$. The following are equivalent.
i. j is basic equation preserving
ii. j is a monomorphism.
iii. j is equation preserving

Proof: Suppose j is basic equation preserving. Then $x = y \leftrightarrow f(x) = f(y)$, and so f is one-one. Also $xy = z \leftrightarrow f(x)f(y) = f(z)$. Setting $z = xy$, we have $f(x,y) = f(x)f(y)$. So j is a monomorphism. Now suppose j is a monomorphism. We need to check that $x_1...x_n = y_1...y_m \leftrightarrow f(x_1)...f(x_n) = f(y_1)...f(y_m)$. By Lemma 1.1.1, this is equivalent to $x_1...x_n = y_1...y_m \leftrightarrow f(x_1...x_n) = f(y_1...y_m)$. This follows immediately from f being one-one. QED

We now introduce some stronger notions of preserving.

DEFINITION 1.1.3. A variable equation in G is an equation where zero or more of the terms are variables and zero or more of the terms are elements of G (parameters). Thus in general, a variable equation uses both variables and parameters from G. A finite set of variable equations in G is solvable if and only if there are choices of elements of G for the variables (same variable must be assigned the same element of G) so that the variable equation becomes a true equation. $j:G \to H$ is solvable equation preserving if and only if every finite set of variable equations in G is solvable in G if and only if it is solvable in H when the parameters from G are replaced by their values under j in H.

DEFINITION 1.1.4. A variable boolean statement in G is a propositional combination of variable equations in G (using not,and,or,implies,iff) where zero or more of the terms are variables and zero or more of the terms are parameters G. A variable boolean statement is solvable in G if and only if there are choices of elements of G for the variables (same variable must be assigned the same element of G) so that the variable boolean statement becomes a true boolean statement. j:G → H is boolean solvable preserving if and only if every variable boolean statement in G is solvable in G if and only if it is solvable in H when the parameters from G are replaced by their values under j in H.

We now introduce a much stronger notion of preserving mappings of G into H, from model theory.

DEFINITION 1.1.5. j:G → H is logic preserving if and only if any first order statement with parameters from G holds in G if and only if it holds over H with the parameters replaced by their values under j. In mathematical logic j is called an elementary embedding from G into H.

DEFINITION 1.1.6. j:G → H is absolutely preserving if and only if for all $x_1,\ldots,x_n \in G$, there is an isomorphism f:G → H such that $j(x_1),\ldots,j(x_n) = f(x_1),\ldots,f(x_n)$.

The strongest notion of all is that j:G → H it an isomorphism. Obviously every isomorphism is absolutely preserving.

THEOREM 1.1.3. Let G be the free abelian (non abelian) group (semigroup) on an infinite set of generators D. There is a non surjective absolutely preserving function on G.

Proof: Let h:D → D be a non surjective one-one map. h naturally induces an isomorphism from G properly into G. G is absolutely preserving but not an isomorphism (not surjective). This is because any one-one function on a finite subset of D extends to a bijection of D. QED

We find it convenient to use a more compact and flexible notation in this paper for most of the notions introduced above.

LIST OF SEVEN PRESERVATION CONDITIONS ON j:G → H
with equivalent names

morphism

equation preserving ↔
monomorphism

solvable equation preserving ↔
E*= preserving

solvable boolean preserving ↔
E*-bool preserving

logic preserving
elementary embedding

absolutely preserving

isomorphism

These are just those preservation conditions that play a role in this initial paper, and here with only G = H.

The idea behind the E*= and E*-bool notation is as follows. The E*= statements in LSG = the language of semigroups, read $(\exists x_1,\ldots,x_k)(\varphi)$ where φ is a finite conjunction of semi group equations which allow parameters (constants) from the semi group. The E*-bool statements in LSG read $(\exists x_1,\ldots,x_k)(\varphi)$ where φ is a propositional combination of semi group equations which allow parameters (constants) from the semi group. Preservation of j:G → G means that the statements are equivalent to the statements when the parameters are replaced by their values under j.

1.2. FOUR EXAMPLES: Z,Z^+,Q,Q^+

DEFINITION 1.3.1. Z is the additive group of integers. Z+ is the additive semi group of positive integers. Q is the additive group of rationals. Q^+ is the additive semi group of positive rationals.

We can determine all of the mappings on each of these four which obey these eight kinds of preservation.

MORPHISM

Z. cx, $c \in Z$.

Z^+. cx, $c \in Z^+$.

Q. cx, $c \in Q$.

Q^+. cx, $c \in Q^+$.

Proof: For Z, let $f(x+y) = f(x)+f(y)$. Then $f(0) = f(0)+f(0)$ and so $f(0) = 0$. By induction on $n \geq 1$, $f(n) = nf(1)$. Also $f(x+-x) = f(x)+f(-x) = f(0) = 0$. Hence $f(-x) = -f(x)$. Therefore for $n \geq 1$, $f(-n) = -f(n) = -nf(1)$. Hence $f(x) = cx$, where $c \in Z$, and any cx is a morphism. Obviously $c = \pm 1$ has cx surjective.

For Z^+, let $f(x+y) = f(x)+f(y)$. By induction on $n \geq 1$, $f(n) = nf(1)$. Hence $f(x) = cx$, where $c \in Z^+$, and any cx, $c \in Z^+$ is a morphism.

For Q, let $f(x+y) = f(x)+f(y)$. Then $f(0) = f(0)+f(0)$, and so $f(0) = 0$. By induction on $n \geq 1$, $f(nx) = nf(x)$. Also $f(x+-x) = f(x)+f(-x) = f(0) = 0$, and hence $f(-x) = -f(x)$. So for $n \in Z$, $f(nx) = nf(x)$. Hence for $n \neq 0$, $f(n(1/n)) = f(1) = nf(1/n)$, and so $f(1/n) = f(1)/n$. Hence for $m \in Z$, $n \in Z+$, $f(m/n) = mf(1)/n = f(1)(m/n)$. Therefore $f(x) = f(1)x$. So f is cx for some $c \in Q$.

For Q^+, let $f(x+y) = f(x)+f(y)$. As before, $f(0) = 0$, and for $n \geq 1$, $f(nx) = nf(x)$. Hence $f(n(1/n)) = nf(1/n) = f(1)$, and so $f(1/n) = f(1)/n$. Hence for $m \geq 0$, $f(m/n) = f(1)m/n$. Hence $f(x) = f(1)x$, and so $f(x) = cx$ for some $c \in Q^+$.

EQUATION PRESERVING MONOMORPHISM

Z. cx, $c \in Z\backslash\{0\}$.

Z^+. cx, $c \in Z^+$.

Q. cx, $c \in Q\backslash\{0\}$.

Q^+. cx, $c \in Q^+$.

Proof: These are the one-one morphisms. For Z, these are the cx, c ≠ 0, and surjective if and only if c = ±1. For Z^+, these are the cx, c ∈ Z^+, and surjective if and only if c = 1. For Q, these are the cx, c ∈ Q, c ≠ 0, all of which are surjective. For Q^+, these are the cx, c ∈ Q^+, all surjective. QED

SOLVABLE EQUATION PRESERVING
E*= PREERVING

SOLVABLE BOOLEAN PRESERVING
E*-bool PRESERVING

LOGIC PRESERVING
ELEMENTARY EMBEDDING

ABSOLUTELY PRESERVING

(all four above categories are the same for Z,Z^+,Q,Q^+)

Z. x and -x.

Z^+. x.

Q. cx, c ∈ Q\{0}.

Q^+. cx, c ∈ Q^+.

Proof: For Z, let f be solvable equation preserving. Then f is cx, c ≠ 0. (∃y)(y+...+y = x) ↔ (∃y)(y+...+y = cx) is obviously false if we use |c| y's and x = 1, |c| > 1. Hence c = ±1. Also x and -x are obviously automorphisms.

For Z^+, let f be solvable equation preserving. Then f is cx, c ∈ Z^+. The rest of the argument is the same as for Z. Also x is obviously an automorphism.

For Q, let f be solvable equation preserving. Then f is cx, c ∈ Q\{0}. And these are all automorphisms.

For Q^+, let f be solvable equation preserving. Then f is cx, c ∈ Q^+. And these are all automorphisms. QED

So our hierarchy of six preservation conditions (including morphism), collapses at solvable equation preserving for the four special cases Z,Z^+,Q,Q^+ in the strong sense that for these four cases, all of the mappings are preserving at that level are already automorphisms. In face, for Q,Q+ it collapses at equation preserving since all of the equation preserving mappings are automorphisms.

There is an obvious more refined catalogue. It is natural to use this more refined hierarchy for $n \geq 1$:

morphism
monomorphism
Σ_n= preserving
Σ_n-bool preserving
elementary embedding
absolutely preserving
automorphism

Let f be a mapping on a semi group G. The behavior of f is the set of items in this refined catalogue in which f lies.

RESEARCH. Let G be a semi group. The behavior set for G is the set of all behaviors of mappings of G. Determine which behavior sets can arise for the various semigroups G. Is there a (natural) semi group whose behavior set is maximum? Address these questions for groups.

1.3. SOME GENERALITIES

DEFINITION 1.3.1. An idempotent in a semi group G is an $x \in G$ with $xx = x$.

THEOREM 1.3.1. Every semi group with an idempotent and more than one element has a non surjective morphism.

Proof: Take $j:G \rightarrow G$ to be constantly any given idempotent. Then j is a non surjective morphism. QED

THEOREM 1.3.2. Every group has an idempotent. Every finite semi group has an idempotent. The semi group of positive integers under addition has no idempotent.

Proof: The identity element of any group is an idempotent. Let G be a finite semi group. Let $x \in G$, and do iterated squaring in G starting with x. Then we obtain some $y = y^k$, k

≥ 2. If k = 2 then we are done. Suppose k ≥ 3. Then $y^{k-1}y^{k-1} = y^{2k-2} = yy^{k-2} = y^{k-1}$, and so y^{k-1} is an idempotent. For the second claim, let j:G → G be constantly any idempotent. QED

THEOREM 1.3.3. Every group and every finite semi group has a non surjective morphism.

Proof: By Theorems 1.3.1 and 1.3.2. QED

1.4. SYMMETRIC SEMIGROUPS

The focus of this paper is on the symmetric semigroups. Sections 2-4 work only with symmetric semigroups.

DEFINITION 1.4.1. The symmetric semigroups are the semigroups DD consisting of all functions from D into D under function composition. We write DD = (DD,•), and we often write DD for just the set without the •.

Note that because of the identity map, all symmetric semigroups are monoids.

In section 2.1 we give the well known characterization of the automorphisms of DD as mappings induced by bijections of D via conjugation.

Let us look at the refined hierarchy from section 1.2 for symmetric semigroups:

morphism
monomorphism
Σ_n= preserving
Σ_n-bool preserving
elementary embedding
absolutely preserving
automorphism

The following remarks pertain **only to symmetric semigroups:**

Here Σ_1= is taken to be the same as E*=, which is the same as solvable equation preserving. Also Σ_1-bool is taken to be the same as E*-bool. This is also the same as solvable equation preserving. Let DD be given. It is immediate that every Σ_1-bool preserving mapping on DD preserves the identity. We show in Lemma 3.2.6 that Σ1= preserving is equivalent to Σ_1-bool preserving. Thus we have that every solvable equation preserving mapping preserves the identity.

There is always a monomorphism that is not surjective and not a monomorphism (map everything to the identity). If the underlying set D is finite then all monomorphisms are obviously automorphisms.

We show in section 2.2 that if the underlying set is infinite, there is a monomorphism that preserves the identity and is not Σ_1= preserving. Now is there a Σ_1= preserving mapping that is not Σ_2= (Π_1=,Σ_1-bool,Π_1-bool) preserving? Is there even a Σ_1= preserving mapping that is not an automorphism?

In this paper we only address the latter question: is there a Σ_1= preserving mapping that is not an automorphism? We show that the answer is yes for certain necessarily extremely large underlying sets D (see section 3.2). Thus it is consistent with the ZFC axioms that for all D, every Σ_1= preserving mapping is an automorphism.

On the other hand, from section 3.2 the existence of DD with a Σ_1= preserving mapping that is not an automorphism is equivalent to a certain large cardinal hypothesis called I2. The methods there show that the existence of DD with a Σ_n= preserving mapping that is not an automorphism is equivalent to obvious extensions of I2 that approach but do not arrive at the stronger large cardinal hypothesis I1. I.e., a nontrivial Π_n elementary embedding of some V(α+1) into V(α+1).

As indicated earlier, by Lemma 3.2.8, any Σ_1= preserving mapping Σ_1-bool preserving and preserves the identity. From its proof, we also see that any Σ_n= preserving mapping is Σ_n-bool preserving.

In section 5 we show that every absolutely preserving mapping of a symmetric semigroup is an automorphism.

2. EQUATION PRESERVING

In this section and in the subsequent sections 3,4, we only consider mappings of the symmetric semigroups.

We write DD ambiguously for the set DD and the symmetric semi group (DD,•).

2.1. SURJECTIVE MAPPINGS

THEOREM 2.1.1. The surjective equation preserving mappings of DD are the same as the semi group automorphisms of DD. They all preserve the identity.

Proof: Let j be a surjective equation preserving mapping of DD. By Theorem 1.1.2, j is a monomorphism. Since j is surjective, j is an isomorphism from DD onto DD; i.e., an automorphism of DD. Now let j be a semi group automorphism of DD. Then j is a surjective monomorphism, and therefore also equation preserving. Note that for all f, fid = f, where id is the identity. Hence for all f, j(f)j(id) = j(f). Since j is onto, we have for all g, gj(id) = g. Setting g to be the identity, idj(id) = id, and so j(id) = id. QED

We now show that the semi group automorphisms of DD are the bijections of DD induced from the bijections of D via conjugation (well known).

DEFINITION 2.1.1. Let $f:D \to D$ be a bijection. Define $[f]:DD \to DD$ by for all $g \in DD$, $[f](g) = f^{-1}gf$.

LEMMA 2.1.2. Let $f:D \to D$ be a bijection. $[f]:DD \to DD$ is an automorphism of DD.

Proof: Let $f:D \to D$ be a bijection. We claim that [f] is a bijection. Suppose [f](g) = [f](h). Then $f^{-1}gf = f^{-1}hf$, and so $ff^{-1}gff^{-1} = ff^{-1}hff^{-1} = g = h$. Thus [f] is one-one. For surjectivity, note that $f^{-1}(fgf^{-1})f = g$. Finally we check that [f] is a morphism. We need [f](gh) = [f](g)[f](h). I.e., $f^{-1}(gh)f = (f^{-1}gf)(f^{-1}hf)$ which is obvious by cancelling the ff^{-1}. QED

DEFINITION 2.1.2. $d^* \in DD$ is constantly d.

LEMMA 2.1.3. Let f be an automorphism of DD. Then f maps the c* one-one onto the c*.

Proof: The c* are the x with the property that $(\forall y)(xy = x)$. This property is preserved under f and f^{-1} as they are automorphisms of (DD,•). QED

LEMMA 2.1.4. Every automorphism of DD is uniquely of the form [f].

Proof: Now let α:DD → DD be an automorphism of DD. By Lemma 2.1.3, α maps the c* one-one onto the c*. Let f:D → D be given as follows. Let x ∈ D. Then αx* is some unique y*, and set f(x) = y. I.e., $\alpha x^* = f(x)^*$, and so $x^* = \alpha f^{-1}(x)^*$. We now show that $\alpha = [f]^{-1} = [f^{-1}]$.

For all x ∈ D, $\alpha(g)(x^*) = \alpha(g)\alpha(f^{-1}(x)^*) = \alpha(gf^{-1}x^*) = \alpha(gf^{-1}x^*) = fgf^{-1}x^* = fgf^{-1}(x)^*$ Hence for all x ∈ D, $\alpha(g)(x) = fgf^{-1}(x)$. Therefore $\alpha(g) = fgf^{-1}$, and hence $\alpha = [f^{-1}]$. QED

THEOREM 2.1.5. The surjective equation preserving mappings of any symmetric semi group are the same as its semi group automorphisms and are uniquely given by [f], f:D → D a bijection, all of which are semigroup automorphisms.

Proof: By Lemmas 2.1.1, 2.1.2, 2.1.4. QED

2.2. NON SURJECTIVE MAPPINGS

THEOREM 2.2.1. Every infinite symmetric semi group has a non surjective equation preserving mapping. We can require that the identity is mapped to itself, and the mapping is not solvable equation preserving.

Proof: Let D be infinite. Let d ∈ D be arbitrary. Let h:D → D\{d} be a bijection, which exists because D is infinite. Define j:DD → DD as follows. Let f ∈ DD. Set j(f)(d) = d and for x ∈ D\{d}, $j(f)(x) = hfh^{-1}(x)$. This uniquely defines j(f). Clearly j(f)(x) ≠ d for x ∈ D\{d} because j(f)(x) is a value of h. Hence j(f) cannot be the constantly d function, and therefore j is not surjective. We claim that j is one-one. Let j(f) = j(g). Then hfh-1 = hgh-1 on D\{d}. Then hf = hg on D. Hence f = g. It remains to verify that j is a morphism. For x ∈ D\{d}, $j(fg)(x) = hfgh^{-1}(x)$ and $j(f)j(g)(x) = j(f)hgh^{-1}(x) = hfh^{-1}(hgh^{-1}(x)) = hfgh^{-1}(x)$. Also j(fg)(d) = d = j(f)j(g)(d). Note j(id)(d) = d, and for x ∈ D\{d}, $j(id)(x) = h(id)h^{-1}(x) = x$. So j(id) = id.

Let f ∈ DD have no fixed point. Then $(\exists x)(f(x) = x) \leftrightarrow (\exists x)(j(f)(x) = x)$ is false because the left hand is false and the right side is true with x = d. So f is not solvable equation preserving. QED

We can restate Theorem 2.2.1 as follows. Note that all symmetric semigroups are in fact monoids where the identity element is the identity function.

THEOREM 2.2.2. Every infinite symmetric semi group has a monomorphism which is not an automorphism, even as a monoid. In fact, every infinite symmetric semi group has a monomorphism which is not solvable equation preserving, even as a monoid.

3. SOLVABLE EQUATION PRESERVING

3.1. DERIVATION FROM I2

Here we prove the existence of a symmetric semi group with a non surjective solvable equation preserving mapping. We use a special large cardinal hypothesis to do this.

Obtaining a symmetric semi group with a non surjective solvable equation preserving mapping, or equivalently, a solvable equation preserving morphism that is not an automorphism, is an entirely different matter than Theorems 2.2.1, 2.2.2 where only equation preserving is featured rather than the much stronger solvable equation preserving.

In fact we show here that this cannot be obtained within the usual ZFC axioms for mathematics. However, we do obtain such using an extremely powerful large cardinal hypothesis known as I2 which is generally believed in the set theory community to be a viable hypothesis to add to ZFC - with some hesitation. In particular, it is believed to be consistent by the set theory community - again with some hesitation. The hesitation surrounds a widely held criteria that there must be some sort of viable "inner model theory" associated with the large cardinal hypothesis before it gains full confidence from that community.

I2 is usually presented as the middle principle in the series I3,I2,I1 in increasing order of strength. See [Ka94], p. 325. The strongest one, I1 figures in section 4, and is also generally believed to the consistent by the set theory community - with the same hesitation.

I1,I3 asserts the existence of certain elementary embeddings from sets into sets, written $j:A \to B$. I2 asserts the existence of a certain elementary embedding from V into a proper class. However, I2 is well known to have equivalent formulations also written $j:A \to B$. It is understood that the elementary embedding goes from $(A,\in)$ into $(B,\in)$. Nontriviality means that j is not the identity function on its domain. The critical point cr(j) is the least ordinal γ such that $j(\gamma) \neq \gamma$. If A is transitive then j is one-one, then $cr(j) < j(cr(j))$, and cr(j) is a limit ordinal.

We always use λ for limit ordinals.

I3. There is a nontrivial elementary embedding $j:V(\lambda) \to V(\lambda)$.
I1. There is a nontrivial elementary embedding $j:V(\lambda+1) \to V(\lambda+1)$.

Ken Kunen famously refuted the following using ZFC, [Ku71]:

There is a nontrivial elementary embedding $j:V(\lambda+2) \to V(\lambda+2)$.

Here is what has become the official version of I2. We discuss some well known variants of I2 here, one of which is most convenient for us: I2''.

I2. There is a nontrivial elementary embedding $j:V \to M$, M a transitive class, and α such that $V(\alpha) \subseteq M$, $j(\alpha) = \alpha > cr(j)$.

Notice that this official formulation is not within set theory, but instead within class theory. Say over the infrastructure NBG + AxC. But it is well known that I2 can be conveniently formulated in many ways in set theory. Here are two such formulations in set theory.

DEFINITION 3.1.1. Let $f:V(\lambda) \to V(\lambda)$. We define $f^+:V(\lambda+1) \to V(\lambda+1)$ by $f^+(A) = \bigcup\{f(B): B \subseteq A \wedge B \in V(\lambda)\}$.

DEFINITION 3.1.2. The Π_1 formulas over $V(\lambda+1)$ are of the form $(\forall A_1,\ldots,A_n \subseteq V(\lambda))(Qx_1\in V(\lambda)\ldots(Qx_m\in V(\lambda))(\varphi)$, with parameters $x_{m+1},\ldots,x_r \in V(\lambda)$ and parameters $A_{n+1},\ldots,A_s \subseteq V(\lambda)$, where the atomic formulas are $x_i = x_j$, $x_i \in x_j$, $x_i \in A_j$. The precise form of this definition is useful near the end of section 3.2.

I2'. There is a nontrivial elementary embedding $j:V(\lambda) \to V(\lambda)$ such that for all well founded relations R on $V(\lambda)$, $j^+(R)$ is well founded.
I2''. There is a nontrivial embedding $j:V(\lambda+1) \to V(\lambda+1)$ that is elementary for Π_1 formulas.

THEOREM 3.1.1. NBG + AxC proves the equivalence of I2,I2',I2'', where ZFC proves the equivalence of I2',I2''. ZFC proves λ witnesses I2' if and only if λ witnesses I2''. ZFC proves that if λ witnesses I2' or I2'' then λ is the least fixed point of j above the critical point of j.

Proof: Well known. See [Ka94]. QED

THEOREM 3.1.2. ZFC + I2'' (or ZFC + I2' or NBG + AxC + I2) prove the existence of a symmetric semi group with a non surjective solvable equation preserving mapping. If there is a nontrivial Π_1 elementary embedding $j:V(\lambda) \to V(\lambda)$ then there is a non surjective solvable equation preserving mapping of $\lambda\lambda$.

Proof: Let $j:V(\lambda+1) \to V(\lambda+1)$ be a nontrivial Π_1 elementary embedding. Let $f \in \lambda\lambda$. Since $V(\lambda+1)$ satisfies that $f:\lambda \to \lambda$, it is clear that M satisfies that $j(f):\lambda \to \lambda$, and so $j(f):\lambda \to \lambda$. Hence $j:\lambda\lambda \to \lambda\lambda$. Let κ be the critical point of j. Let $i(\kappa)$ be the element of $\lambda\lambda$ that is constantly κ. We claim that $i(\kappa)$ cannot be a value of j. For if $j(f) = i(\kappa)$ then $j(f)$ is constant, and so f is constant. Now $j(f)(0) = i(\kappa)(0) = \kappa = j(f)(j(0)) = j(f(0))$. Since $\kappa \notin rng(j)$, we have a contradiction.

It remains to show that j is E*= preserving. Let ψ be the existential statement $(\exists f_1,\ldots,f_k:V(\lambda) \to V(\lambda))(\varphi)$, where φ is a finite set of equations in variables $f_1,\ldots,f_k$ and parameters $g_1,\ldots,g_m:\lambda \to \lambda$. This is a Σ_1 formula over $V(\lambda+1)$, and so it is preserved when we pass from $g_1,\ldots,g_m$ to $j(g_1),\ldots,j(g_m)$. QED

It is immediate from this construction that the identity is preserved - although by Lemma 3.2.8 we know that it is automatic for symmetric semigroups.

It will be convenient to introduce the following terminology.

DEFINITION 3.1.3. An I1 ordinal is an ordinal α such that there is a nontrivial elementary embedding $j:V(\alpha+1) \to V(\alpha+1)$. An I2 ordinal is an ordinal α such that there is a nontrivial Π_1 elementary $j:V(\alpha+1) \to V(\alpha+1)$. An I3 ordinal is an ordinal α such that there is a nontrivial elementary $j:V(\alpha) \to V(\alpha)$.

THEOREM 3.1.3. The following holds.
1. The I1 cardinals are the same as the I1 ordinals and the I1 ω limits of strongly inaccessible cardinals.
2. The I2 cardinals are the same as the I2 ordinals and the I2 ω limits of strongly inaccessible cardinals.
3. The I3 cardinals are the same as the I3 limit ordinals and the I3 ω limits of strongly inaccessible cardinals.
4. The I3 successor ordinals are the same as the successors of the I1 ordinals.

Proof: We use κ for critical points of embeddings. We first establish the following claim *). Let $j:V(\lambda) \to V(\lambda)$ be a nontrivial elementary embedding. Let μ be the limit of the iterates of j at κ. It is well known that κ is a strongly inaccessible cardinal, and so its iterates are, and therefore μ is an ω limit of strongly inaccessible cardinals. If $\mu = \lambda$ then we are done. Otherwise, $\kappa < \mu < \lambda$, and obviously $j(\mu) = \mu$, and so each $j(\mu+n) = \mu+n$. Hence $j:V(\mu+2) \to V(\mu+2)$ is a nontrivial elementary embedding, running into the Kunen inconsistency.

For 1, let $j:V(\alpha+1) \to V(\alpha+1)$ be a nontrivial elementary embedding. If α is a successor then $j:V(\beta+2) \to V(\beta+2)$ is a nontrivial elementary embedding, and we run into the Kunen inconsistency. Hence α is a limit, and in particular $j:V(\alpha) \to V(\alpha)$ is a nontrivial elementary embedding. By *), α is an ω limit of strongly inaccessible cardinals.

For 2, let $j:V(\alpha+1) \to V(\alpha+1)$ be a nontrivial $\Pi 1$ elementary embedding. If α is a successor then $j:V(\beta+2) \to V(\beta+2)$ is a nontrivial $\Pi 1$ elementary embedding. We still run into the Kunen inconsistency using ω-Jonsson because we only need a parameter from $V(\beta+2)$ and quantification over $V(\beta+1)$, let alone Π_1 over $V(\beta+2)$. Hence α is a limit, and we proceed as above for 1.

For 3, let $j:V(\lambda) \to V(\lambda)$. By *), λ is an ω limit of strongly inaccessible cardinals.

For 4, let $\alpha+1$ be an I3 ordinal. Then obviously α is an I1 ordinal. Let α be an I1 odinal. Then obviously $\alpha+1$ is an I3 ordinal. QED

In Theorem 3.1.3, using "ω limits of strongly inaccessible cardinals" is useful in working with the $V(\alpha)$'s in Theorem 3.2.49. Of course more can be said, like "ω limits of measurable cardinals", and so forth.

We can now restate Theorem 3.1.2.

THEOREM 3.1.4. If λ is an I2 cardinal then there is a non surjective solvable equation preserving mapping of $\lambda\lambda$.

Proof: According to the proof of Theorem 3.1.2. QED

3.2. DERIVATION OF I2

We now start with a non surjective E*= preserving mapping j on a symmetric semi group DD. We derive I2. I.e., j is solvable equation preserving.

In this section 3.2 we use five languages, LSG, LUF, LMF, LMFR, BL2. The first language is language of semigroups, LSG. It has only the binary object • for composition (equality is always taken for granted). The first four of these languages will be applied only to one specific structure built from the set D. In the case of LSG we apply it only to the semi group (D,•). Since we are using multiple languages, it is convenient to tie our notions of E*= explicitly to these five languages, which for now is LSG. Thus we henceforth say that j is E*=/LSG preserving. Later related notions will be tied to the later languages.

The first major goal is to show that j is E*-bool/LSG preserving. We begin this proof with some results that do not involve the mapping j, and apply to all symmetric semigroups DD.

DEFINITION 3.2.1. The formulas of LSG are the usual formulas in one binary function symbol • with equality. The statements of LSG are the formulas of LUF where the free occurrences of variables of φ ranging over D (DD) have all been replaced by elements of DD. The formula statements of LUF are the formulas of LUF where zero, some, or all of the free occurrences of variables of φ have all been replaced by elements of DD. The objects that replace free occurrences in statements and formula statements are called the parameters of the statements and formula statements, respectively. It is required that all free occurrences of the same variable either do not get replaced or get replaced by the same element of DD. A*=/LSG/fm, A*=/LSG/st, A*=/LSG/fmst is the set of all formulas, statements, formula statements that begin with zero or more universal quantifiers, followed by a finite conjunction of equations. E*=/LSG/fm, E*=/LSG/st, E*=/LSG/fmst are the same with "universal" replaced by "existential". A*-bool/LSG/fm, A*-bool/LSG/st, A*-bool/LSG/fmst is the set of all formulas, statements, formula statements that begin with zero or more universal quantifiers, followed by a propositional combination of equations. E*-bool/LSG/fm, E*-bool/LSG/st, E*-bool/LSG/fmst are the same with "universal" replaced by "existential".

DEFINITION 3.2.2. We use j1:DD → DD for the fixed E*=/LSG preserving mapping on the symmetric semi group DD. More generally, for the various statement classes K, K/LSG preserving means that every statement in K holds if and only if it holds if the parameters are replaced by their values under j1. Until we introduce our third language LMF much later in this section 3.2, we use f,g,h,F,G,H, with and without subscripts and superscripts ',*, for elements of DD, unless indicated otherwise. We use a,b,c,d,u,v,w,x,y,z, with and without subscripts and superscript ', for elements of D, unless indicated otherwise. For d ∈ D, d* ∈ DD is constantly d. C = {d*: d ∈ D}.

The reason that we write j_1 here and not j here is that we are looking forward to later defining a related map $j_0:D \to D$.

LEMMA 3.2.1. Let $rng(F) \cap rng(G) = \emptyset$. Let $f \neq g$.
i. $(\exists h,d)(hf(d) \in rng(F) \wedge hg(d) \in rng(G))$.
ii. $(\exists h,d,F',G')(hfd^* = FF' \wedge hgd^* = GG')$.
iii. $(\exists h,H,F',G')(hfH = FF' \wedge hgH = GG')$.

Proof: For i, let F,G be as given and $f \neq g$. Let $f(d) \neq g(d)$. Let h send f(d) into rng(F) and g(d) into rng(G).

For ii, we use the same h,d, so that hfd^* is constantly a value of F and hgd^* is constantly a value of G. Now obviously any constant value of F is the result of applying some (constant) function first followed by F, and any constant value of G is the result of applying some (constant) function first followed by G.

For iii, simply use $H = d^*$. QED

LEMMA 3.2.2. There is an E*=/LSG formula statement with free variables f,g and two parameters, which defines $f \neq g$, as long as the two parameters have disjoint ranges.

Proof: Use Lemma 3.2.1iii. We need to check that iii is false if $f = g$. Let $hfH = FF' \wedge hfH = GG'$ and $d \in D$ be arbitrary. Then $hfH(d) = FF'(d) \wedge hfH(d) = GG'(d)$, and so F,G have a common value, hfH(d), which is impossible. QED

LEMMA 3.2.3. Every boolean formula with variables among $f_1,...,f_n$ is equivalent to a disjunction of E*= formula statements with free variables among $f_1,...,f_n$, with any two parameters (for the entire disjunction) with disjoint ranges. The choice of formula is independent of the choice of such parameters.

Proof: Let $\varphi,f_1,...,f_n$ be as given. Put φ in disjunctive normal form, as $\psi_1 \vee ... \vee \psi_r$. Write ψ_i in the form $\rho_i \wedge s_1 \neq t_1 \wedge ... \wedge s_p \neq t_p$, where ρ_i is a conjunction of equations and $s_1,...,s_p,t_1,...,t_p$ are terms of LSG, where all variables are among $f_1,...,f_n$. By Lemma 3.2.2, we can write ψ_i as an E*= formula statement with free variables among $f_1,...,f_n$ with the help of any two parameters with disjoint ranges, independently of the choice of those parameters. We then get our length r disjunction of E*= formulas with free variables among $f_1,...,f_n$ with any two parameters with disjoint ranges, again independently of the choice of those two parameters. QED

LEMMA 3.2.4. Every E*-bool formula with free variables among $f_1,...,f_n$ is equivalent to a disjunction of E*= formula statements with free variables among $f_1,...,f_n$, and any two parameters (for the entire disjunction) with disjoint ranges. The choice of formula is independent of the choice of parameters.

Proof: We apply Lemma 3.2.3 to the boolean part of the E*-bool formula with variables among $f_1,...,f_n,g_1,...,g_m$, and then existentially quantify out by $g_1,...,g_m$, to get what is required of the form $(\exists g_1,...,g_m)(\rho_1 \vee ... \vee \rho_r)$, where each ρ_i is E*= again with the help of any two parameters with disjoint ranges, independently of the choice of those parameters. But this is equivalent to $(\exists g_1,...,g_m)(\rho_1) \vee ... \vee (\exists g_1,...,g_m)(\rho_r)$. QED

LEMMA 3.2.5. j_1 is one-one. D is infinite. rng(f),rng(g) meet if and only if $(\exists F,G)(fG = gG)$. f,g have disjoint ranges if and only if $j_1(f),j_1(g)$ have disjoint ranges.

Proof: Let $j_1(f) = j_1(g)$. Then by equation preserving, f = g. Since $j_1:DD \rightarrow DD$ is not surjective, DD is infinite, and so D is infinite. Now let $a,b \in D$ be distinct. $\neg$(f,g have disjoint ranges) $\leftrightarrow$ $(\exists F,G)(fF = gG)$. To see this, suppose $\neg$(f,g have disjoint ranges), and let f(a) = g(b). Then fa* = gb*, and so $(\exists F,G)(fF = gG)$. Now suppose fF = Gg. Let $d \in D$ be arbitrary. Then fF(d) = Gg(d), and $fF(d) \in rng(f)$, and $Gg(d) \in rng(g)$. The third claim follows immediately from the second claim by applying E*= preserving. QED

LEMMA 3.2.6. j_1 is E*-bool/LSG preserving. j_1 is A*-bool/LSG preserving.

Proof: Let φ be an E*-bool/LSG statement $(\exists g_1,...,g_r)(\varphi)$ with parameters $f_1,...,f_n$. By Lemma 3.2.3 let φ be equivalent to a disjunction $\tau_1 \vee ... \vee \tau_r$ of E*= statements with parameters $f_1,...,f_n$,a*,b*, where $a \neq b$ are arbitrary. Note that $a^* \neq b^*$ have disjoint ranges. Suppose φ holds with parameters $f_1,...,f_n$. Let τ_i hold with parameters

$f_1,...,f_n,a^*,b^*$. By E*=/LSG preserving, τ_i holds with parameters $j_1(f_1),...,j_1(f_n),j_1(a^*),j_1(b^*)$. According to Lemma 3.2.5, $j_1(a^*),j_1(b^*)$ have disjoint ranges. Also $\tau_1 \vee ... \vee \tau_n$ holds with parameters $j_1(f_1),...,j_1(f_n),j_1(a^*),j_1(b^*)$, and so φ holds with parameters $j_1(f_1),...,j_1(f_n)$, as we have independence of the choice of parameters in Lemma 3.2.4. Conversely, suppose φ holds with parameters $j_1(f_1),...,j_1(f_n)$. Let τ_i hold with parameters $j_1(f_1),...,j_1(f_n),j_1(a^*),j_1(b^*)$, again using the independence of the choice of parameters in Lemma 3.2.4. By E*= preserving, τ_i holds with parameters $f_1,...,f_n,a^*,b^*$, and so φ holds with parameters $f_1,...,f_n$. Basically we keep using the independence of the choice of parameters (as long as they have disjoint ranges). j_1 is also A*-bool/LSG preserving by taking negations (duality). QED

So we have achieved the first major goal with Lemma 3.2.6.

The following Lemma does not involve j.

LEMMA 3.2.7. Let $a,b \in D$ be distinct. The following holds.
i. id is the unique g such that $(\forall f)(fg = f)$
ii. id is the unique g such that $(\forall f)(gf = f)$
iii. f is constant if and only if $(\forall g)(fg = f)$
iv. f is constant if and only if $(\exists g)(f = ga^*)$
v. f is one-one if and only if $(\exists g)(gf = id)$
vi. f is onto if and only if $(\exists g)(fg = id)$
vii. f is a bijection if and only if $(\exists g)(fg = gf = id)$
viii. $f \neq g \leftrightarrow (\exists F,G)(FfG = a^* \wedge FgG = b^*)$

Proof: i. id obviously has the property. Suppose $(\forall f)(fg = f)$. Setting f = id, we get idg = id, and so g = id.
ii. id obviously has the property. Suppose $(\forall f)(gf = f)$. Setting f = id, we get gid = id, and so g = id.
iii. The forward direction is obvious. Suppose $(\forall g)(fg = f)$, and let $c \neq d$. Then $fc^* = f(c)^* = f = fd^* = f(d)^*$, and so $f(c) = f(d)$.
iv. If f is constantly b then $f = ga^*$ provided $g = b^*$. Suppose $f = ga^*$. Then f is constant.
v. Suppose f is one-one. Choose g so that at every $b \in rng(f)$, $g(f(b)) = b$. Hence gf = id. Now suppose gf = id. Let $f(b) = f(c)$. Then $g(f(b)) = b = g(f(c)) = c$. Hence f is one-one.

vi. Suppose f is onto. Choose g so that at b it is some c such that f(c) = b. So f(g(b)) = b, and so fg = id. Now suppose fg = id. Then for all d, fgd* = d*, and so f(g(d)) = d, and d ∈ rng(f).
vii. f is a bijection if and only if f is one-one and onto if and only if (∃g)(gf = id) ∧ (∃g)(fg = id). Note that we can choose the same g = f-1, obtaining (∃g)(fg = gf = id).
viii. Suppose f ≠ g. Let f(c) ≠ g(c). Choose F such that Ff(c) = a ∧ Fg(c) = b. Set G = c*. Then FfG = a* ∧ FgG = b*. Now let FfG = a* ∧ FgG = b*. Then fG ≠ gG. Hence f ≠ g.

QED

LEMMA 3.2.8. The following holds.
i. j_1(id) = id
ii. f is constant if and only if j_1(f) is constant
iii. f is one-one if and only if j_1(f) is one-one
iv. f is onto if and only if j_1(f) is onto
v. f is a bijection if and only if j_1(f) is a bijection

Proof: i. By A*-bool/LSG preserving, (∀f)(fid = f) ↔ (∀f)(fj_1(id) = f). Hence (∀f)(fj_1(id) = f). By Lemma 3.2.7i, j_1(id) = id.
ii. By A*-bool/LSG preserving and Lemma 3.2.7iii.
iii. By Lemma 3.2.7v and E*-bool/LSG preserving, f is one-one ↔ (∃g)(gf = id) ↔ (∃g)(gj_1(f) = j_1(id)) ↔ (∃g)(gj_1(f) = id) ↔ j_1(f) is one-one using Lemma 3.2.7v.
iv. By Lemma 3.2.7vi and E*-bool/LSG preserving, f is onto ↔ (∃g)(fg = id) ↔ (∃g)(j_1(f)g = j_1(id)) ↔ (∃g)(j_1(f)g = id) ↔ j_1(f) is onto using Lemma 3.2.7vi.
v. This follows from iii,iv here.

QED

DEFINITION 3.2.3. v:C → D is given by v(d*) = d. j_0(d) = v(j_1(d*)). This defines j_0:D → D in addition to the original j_1:DD → DD.

LEMMA 3.2.9.
1. f ∈ C ↔ j_1(f) ∈ C.
2. j_0:D → D is well defined.
3. j_1(a*) = j_0(a)*
4. j_0:D → D is one-one.
5. fa* = f(a)*
6. f(b) = v(f(b*))

7. $g \in C \rightarrow f(v(g)) = v(fg)$
8. $j_0(f(a)) = j_1(f)(j_0(a))$.
9. $j_0:D \rightarrow D$ is not onto.
10. Some $a^* \notin rng(j_1)$.

Proof: 1 is by Lemma 3.2.81i. For 2, $v(j_1(a^*))$ is well defined by 1. For 3, $j_0(a) = v(j_1(a^*))$ by definition, and so $j_0(a)^* = j_1(a^*)$. For 4, $j_0(a) = j_0(b) \rightarrow v(j_1(a^*)) = v(j_1(b^*)) \rightarrow j_1(a^*) = j_1(b^*) \rightarrow a^* = b^* \rightarrow a = b$ using that $j_1:DD \rightarrow DD$ is one-one. For 5, $fa^*(b) = f(a)$, and $f(a)^*(b) = f(a)$. For 6, $v(f(b^*)) = v(f(b)^*) = f(b)$, using 5. For 7, let $g = d^*$. Then $f(v(g)) = f(d) = v(f(d^*)) = v(fg)$ using 6. For 8,

a. $j_1(f)(j_0(a))$ =
b. $j_1(f)(v(j_1(a^*))$ =
c. $v(j_1(f)j_1(a^*))$ =
d. $v(j_1(fa^*))$ =
e. $v(j_1(f(a)^*))$ =
f. $v(j_0(f(a))^*)$ =
g. $j_0(f(a))$

b is by definition of j_0. c is by 7 with $g = j_1(a^*)$ and f there is $j_1(f)$ here. d is by j_1 being a morphism. e is by 5. f is by 3. g is by the definition of v.

For Lemma 9, suppose $j_0:D \rightarrow D$ is onto. We claim that $j_1(f) = j_0fj_0^{-1}$. To see this we show that both sides have the same values at any $j_0(a)$, $a \in D$, because $j_1(f)(j_0(a)) = j_0fj_0^{-1}(j_0(a)) = j_0(f(a))$ by 8. Since $j_0:D \rightarrow D$ is onto, two function f,g having the same values at any $j_0(a)$ is sufficient for $f = g$. Now $j_0fj_0^{-1}$ is onto DD, as a function of f, because we can solve $j_0fj_0^{-1} = g$ by setting $f = j_0^{-1}gj_0$. Hence $j_1:DD \rightarrow DD$ is onto, which is a contradiction.

For 10, since $j_0:D \rightarrow D$ is not onto, let $a \notin rng(j_0)$. If $a^* \in rng(j_1)$ then write $a^* = j_1(f)$, and by 1, set $f = b^*$. Then $a^* = j_1(b^*)$ and so $j_0(b) = v(a^*) = a$, contradicting $a \notin rng(j_0)$. QED

We now introduce our second language, LUF (language of unary functions). It will properly extend LSG.

DEFINITION 3.2.4. LUF (language of unary functions) is the language with two sorts D,DD. We use variables v_i, $i \geq 1$, over D, and function variables f_i over DD. We will only work with the specific LUF structure M = (D,DD,•,A) where • is composition from DD^2 into DD, and A is application from DD × D into D. We usually omit the • as we did in LSG (e.g., fg = f•g), and we always omit the A (e.g., f(x) = A(f,x)). The terms are the $f_1f_2...f_k$, $f_1f_2...f_n(x)$, where k ≥ 1 and n ≥ 0. The former has sort DD and the latter has sort D. The atomic formulas are of the form s = t, where s,t are terms of the same sort. The formulas are generated by the atomic formulas by propositional connectives, and quantification over the sorts as usual.

DEFINITION 3.2.5. We distinguish between formulas, statements, and formula statements in LUF. We have already defined the formulas of LUF. The statements of LUF are the formulas of LUF where the free occurrences of variables of φ ranging over D (DD) have all been replaced by elements of D (DD). The formula statements of LUF are the formulas of LUF where zero, some, or all of the free occurrences of variables of φ ranging over D (DD) have all been replaced by elements of D (DD). The objects that replace free occurrences in statements and formula statements are called the parameters of the statements and formula statements, respectively. It is required that all free occurrences of the same variable either do not get replaced or get replaced by the same element of D ∪ DD.

DEFINITION 3.2.6. We continue to use a,b,c,d,u,v,w,x,y,z, with and without subscripts and ', for elements of D, unless indicated otherwise. We use f,g,h, with and without subscripts and ', for elements of DD, unless indicated otherwise. A*=/LUF/fm, A*=/LUF/st, A*=/LUF/fmst is the set of all formulas, statements, formula statements that begin with zero or more universal quantifiers of either sort, followed by a finite conjunction of equations. E*=/LUF/fm, E*=/LUF/st, E*=/LUF/fmst are the same with "universal" replaced by "existential". A*-bool/LUF/fm, A*-bool/LUF/st, A*-bool/LUF/fmst is the set of all formulas, statements, formula statements that begin with zero or more universal quantifiers of either sort, followed by a propositional combination of equations. E*-bool/LUF/fm, E*-bool/LUF/st, E*-bool/LUF/fmst are the same with "universal" replaced by "existential".

DEFINITION 3.2.7. j_0,j_1 is K/LUF preserving if and only if any element of K/LUF/st holds if and only if it holds with all parameters replaced by their values under j_0,j_1. Here K is any of A*=/LUF, E*=/LUF, A*-bool/LUF, E*-bool/LUF.

We will commonly apply K/LUF preserving not only to elements of E/LUF/st but also to elements of E/LUF/fmst. Namely we have truth preservation when we apply j_0,j_1 to the parameters in statements, but also apply j_0,j_1 to the free variables. Of course it doesn't literally make sense to apply j_0,j_1 to a variable, but only to assignments to them. When free variables of formula statements are assigned elements of D ∪ DD, the formula statement becomes a statement.

So why have formulas, statements, and formula statements in the first place and not just formulas and statements? Conceptually it is quite useful. For the parameters we generally used are specially chosen elements of DD over and over again, and always have special properties that are preserved under j_1. Nothing like that is true when we convert formula statements to statements to apply K/LUF preserving. For example, in Lemma 3.2.7iv the existential definition we give for "f is constant". It uses a parameter a*. But 'a' is arbitrary and the same definition will work with any b* and in particular with j(a*) = j(a)*. That is why we get Lemma 3.2.8ii. Here a* and the variable f are treated both as parameters for the E*=/LUF preserving.

LEMMA 3.2.10. j_0,j_1 is E*-bool/LUF, A*-bool/LUF preserving.

Proof: Let $\varphi = (\exists f_1,\ldots,f_n)(\exists a_1,\ldots,a_m)(\psi)$ be an E*-bool/LUF statement with parameters $g_1,\ldots,g_r,b_1,\ldots,b_s$. Let $\varphi_1 = (\exists f_1,\ldots,f_n)(\exists h_1,\ldots,h_m)(h_1,\ldots,h_m \in C \wedge \psi_1)$ be obtained from φ by replacing each occurrence of a_i in ψ by h_i, and with the parameters $g_1,\ldots,g_r,b_1^*,\ldots,b_s^*$, where $b_1,\ldots,b_s$ are replaced by $b_1^*,\ldots,b_s^*$. Now φ_1 can be put in E*-bool/LUF/st using Lemma 3.2.7iv with an arbitrary additional parameter d*, and thus we are using the parameters $g_1,\ldots,g_r,b_1^*,\ldots,b_s^*,d^*$. Then evidently $\varphi \leftrightarrow \varphi_1$ holds and $\varphi_1 \in$ E*-bool/LUF/st. Since j_1 is E*=/LUF preserving, we have $\varphi_2 = (\exists f_1,\ldots,f_n)(\exists h_1,\ldots,h_m)(h_1,\ldots,h_m \in C \wedge \psi_2)$ where we have replaced the parameters $g_1,\ldots,g_r,b_1^*,\ldots,b_s^*,a^*$ by the parameters $j_1(g_1),\ldots,j_1(g_r),j_1(b^*),\ldots,j_1(bs^*),j_1(a^*)$ which are $j_1(g_1),\ldots,j_1(g_r),j_0(b_1)^*,\ldots,j_0(bs)^*,j_0(a)^*$. Then φ_2 is equivalent to $\varphi_3 = (\exists f_1,\ldots,f_n)(\exists a_1,\ldots,a_m)(\psi_3)$ with parameters $j_1(g_1),\ldots,j_1(g_r),j_0(b_1),\ldots,j_0(b_s)$, where we have removed $h_1,...,h_m \in C$ (in the form given by Lemma 3.2.7iv) and replaced $h_1,...,h_m$ by $a_1,...,a_m$. φ_3 is the same as φ with parameters $g_1,...,g_r,b_1,...,b_s$. replaced by $j_1(g_1),...,j_1(g_r),j_0(b_1),...,j_0(b_s)$. QED

DEFINITION 3.2.8. $f^{-1}(a) = \{x:f(x) = a\}$.

$f^{-1}(x) \cap g^{-1}(y) \neq \emptyset$ is obviously E*-bool/LUF in free variables x,y,f,g without any parameters. Our next big goal is to show that $f^{-1}(x) \cap g^{-1}(y) \neq \emptyset$ is A*-bool/LUF in certain parameters. We want the parameters to be strategically chosen so that the definition remains valid even if we change the parameters to "similar parameters". We will use a lot of parameters and we set up what we call the active parameter facility (see below). The treatment of $f^{-1}(x) \cap g^{-1}(y) \neq \emptyset$ will be needed to handle pairing properly just from our j_0,j_1 being E*-bool/LUF preserving.

DEFINITION 3.2.9. $R(h_1,h_2,h_3,h_4,H)$ if and only if h_1,h_2,h_3,h_4 are one-one, $rng(h_1),rng(h_2),rng(h_3),rng(h_4)$ partition D, and $(\forall x)(h_1(H(x)) = x \vee h_2(H(x)) = x \vee h_3(H(x)) = x \vee h_4(H(x)) = x)$.

We will be maintaining a list of what we call the active parameters. These specific objects (elements of D ∪ DD) come with a list of requirements called the parameter requirements. These requirements generally involve several of the active parameters at once, rather than simply being imposed individually.

The alternative parameters are any alternative list of parameters which obey the parameter requirements. The whole point of this active parameter setup is that we look for definitions that need the help of the active parameters and which remain valid (or closely related) when we use any alternative parameters. Thus we have to choose strategic active parameters with strategic parameter requirements. From time to time we release active parameters so we can discard what is no longer needed.

DEFINITION 3.2.10. The currently active parameters comprise a list of 14 chosen elements of D ∪ DD that meet the parameter requirements. The 14 (currently) active parameters are $h_1,h_2,h_3,h_4,H,a_0,a_1,F_1,F_2,F_3,F_4,F_5,F_6$,id with the following parameter requirements.
i. $a_0 \neq a_1$ from D.

ii. $R(h_1,h_2,h_3,h_4,H)$.
iii. $F_1(a_0) = a_0 \wedge (\forall x)(x \neq a_0 \rightarrow F_1(x) = a_1)$.
iv. $F_2(a_1) = a_1 \wedge (\forall x)(x \neq a_1 \rightarrow F_2(x) = a_0)$.
v. F_3 is the identity on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_1 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
vi. F_4 is the identity on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_0 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
vii. F_5 is constantly a_0 on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_1 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
viii. F_6 is constantly a_0 on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_0 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
ix. id is a (the) identity function.

LEMMA 3.2.11. The 14 active parameters in Definition 3.2.10 exist and obey the parameter requirement. The parameter requirement is in A*-bool/LUF/fm.

Proof: For the first claim let $A_1,A_2,A_3,A_4 \subseteq D$ partition D, $|A_1|,|A_2|,|A_3|,|A_4| = |D|$, and let $rng(h_1) = A_1$, $rng(h_2) = A_2$, $rng(h_3) = A_3$. $rng(h_4) = A_4$. For each x let H(x) witness $x \in rng(hi)$. Then $R(h_1,h_2,h_3,h_4,H)$. Let $a_0 \neq a_1$ be arbitrary and let F_1,F_2,id be uniquely defined by iii,iv,ix. Also let F_3 - F_6 be uniquely defined by v-viii.

To see that ii is A*-bool/LUF/fm, the first and third conjuncts in Definition 3.2.9 are obviously A*-bool/LUF/fm. For the second conjunct, the disjointness is obviously A*-bool/LUF/fm. But the union being all of D follows from the third conjunct. The remaining i,iii-ix are clearly A*-bool/LUF/fm. QED

Below we introduce partial functions $J_1,J_2,J_3:DD^4 \rightarrow DD^2$, which we view as 6-ary relations on DD. We are really interested only in J_3, but for greater clarity, we break the construction of J_3 down into J_1,J_2,J_3.

DEFINITION 3.2.11. $J_1(f,g,a,b)$ is defined if and only if $a \neq b$, and is (f_1,g_1), where f_1 is the result of changing all values of f that are a to a_0, all values of f that are not a to a_1, and g_1 is the result of changing all values of g that are b to a_1, and all values of g that are not b to a_0. $J_2(f,g,a,b) = (f_2,g_2)$ is the result of making four copies of each of f_1,g_1 onto the four sets $rng(h_1),rng(h_2),rng(h_3),rng(h_4)$, which has the effect of converting the domain D to A_1,A_2,A_3,A_4, and not affecting values. This is just $f_2 = f_1H$ and $g_2 = g_1H$. $J_3(f,g,a,b) =$

(f_3,g_3) is the result of changing f_2,g_2 on $rng(h_2),rng(h_3),rng(h_4)$, by making f_3 constantly a_0 on $rng(h_2)$, constantly a_1 on $rng(h_3)$, constantly a_1 on $rng(h_4)$, and g_3 constantly a_0 on $rng(h_2)$, constantly a_0 on $rng(h_3)$, and constantly a_1 on $rng(h_4)$. Note that f_3,g_3 are uniquely defined on A_2,A_3,A_4 but remain the same as f_2,g_2 on A_1.

Thus the definition of J_1,J_2,J_3 uses the 14 active parameters. J_3 itself depends solely on the choice of active parameters h_1,h_2,h_3,h_4,H, even though its definition uses more. Moreover we shall see that J_1,J_2,J_3 each have E*-bool/LUF/fmst definitions with are correct for all alternative parameters.

LEMMA 3.2.12. J_1 is E*-bool/LUF/fmst in free variables f,g,a,b,f_1,g_1 with the 14 active parameters, where the definition is correct for all alternative parameters. If $a \neq b$ then $f^{-1}(a) \cap g^{-1}(b) = \emptyset \leftrightarrow J_1(f)^{-1}(a_0) \cap J_1(g)^{-1}(a_1) = \emptyset$.

Proof: To construct $J_1(f,g,a,b) = (f_1,g_1)$, we first convert values a,b to values a_0,a_1, and then apply F_1,F_2. The first step is obviously Gf,Gg, where G is any one-one map sending a to a_0 and b to a_1. Then we take $f_1 = F_1Gf$ and $g_1 = F_2Gf$. We need that $f^{-1}(a) \cap g^{-1}(b) = \emptyset$ gets preserved in this process. The places where f is 'a' are the same as the places where f_1 is 'a_0' (this is not generally true for b,a_1), and the places where g is 'b' are the same as the places where g_1 is a_1 (this is not generally true for a,a_0). And we only care about the case $a \neq b$. This establishes the second claim. So we define $J_1(f,g,a,b) = (f_1,g_1) \leftrightarrow a \neq b \wedge (\exists G)(G \text{ is one-one} \wedge G(a) = a_0 \wedge G(b) = a_1 \wedge f_1 = F_1Gf \wedge g_1 = F_2Gf)$. This is E*-bool/LUF using the parameter id by Lemma 3.2.7v. QED

LEMMA 3.2.13. J_2 is E*-bool/LUF/fmst in free variables f,g,a,b,f_2,g_2 with the 14 active parameters, where the definition is correct in all alternative parameters. If $a \neq b$ then $f^{-1}(a) \cap g^{-1}(b) = \emptyset \leftrightarrow J_2(f,g,a,b)_1{}^{-1}(a_0) \cap J_2(f,g,a,b)_2{}^{-1}(a_1) \cap rng(h_1) = \emptyset$.

Proof: $J_2(f,g,a,b) = (f_1H,g_1H)$. f_1H,g_1H restricted to $rng(h_i)$ is a copy of f_1,g_1, respectively, under a one-one shrinking of the domain D to the altered domain $rng(h_i)$. Hence for all i, $f_1{}^{-1}(a) \cap g_1{}^{-1}(b) = \emptyset \leftrightarrow J_2(f,g,a,b)_1{}^{-1}(a_0) \cap J_2(f,g,a,b)_2{}^{-1}(a_1) \cap rng(h_i) = \emptyset$. We need this only for $i = 1$. Apply the second claim of Lemma 3.2.12. Also $J_2(f,g,a,b) = (f_2,g_2) \leftrightarrow$

$(\exists f_1,g_1)(f_2 = f_1H \wedge f_2 = g_1H \wedge J_1(f,g,a,b) = (f_1,g_1))$ which is clearly E*-bool/LUF. QED

LEMMA 3.2.14. J_3 is E*-bool/LUF/fmst in free variables f,g,a,b,f_3,g_3 with the 14 active parameters, where the definition is correct in all alternative parameters. If $a \neq b$ then $f^{-1}(a) \cap g^{-1}(b) = \emptyset \leftrightarrow J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_1) = \emptyset$. Moreover, $J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_1)$ have cardinality $|D|$.

Proof: $J_3(f,g,a,b) = (f_3,g_3) \leftrightarrow f_3 = F_3f_2 \wedge g_3 = F_4g_2$. Note that application of F_3,F_4 retain all the information from J2(f,g,a,b) on $rng(h_1)$, and cleanse all the information from J2(f,g,a,b) on $rng(h_2),rng(h_3),rng(h_4)$. In particular all common elements of $J_2(f,g,a,b)_1{}^{-1}(a_0),J_2(f,g,a,b)_2{}^{-1}(a_1)$ in $rng(h_2),rng(h_3),rng(h_4)$ are removed. So $J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_1) = J_2(f,g,a,b)_1{}^{-1}(a_0) \cap J_2(f,g,a,b)_2{}^{-1}(a_1)$. The three intersections in the last claim are respectively $rng(h_2),rng(h_3),rng(h_4)$, all of which have cardinality $|D|$. $J_3(f,g,a,b) = (f_3,g_3) \leftrightarrow (\exists f_2,g_2)(f_3 = F_3f_2 \wedge g_3 = F_4g_2 \wedge J_2(f,g,a,b) = (f_2,g_2))$ which is clearly E*-bool/LUF. QED

Now the point of F_5,F_6 is to give two functions in the active parameters, which would mimic the structure of $J_3(f,g,a,b)$ if and only if $f^{-1}(a) \cap g^{-1}(b) = \emptyset$. Thus $f^{-1}(a) \cap g^{-1}(b) = \emptyset$ is equivalent to F_5,F_6 mimics $J_3(f,g,a,b)$.

LEMMA 3.2.15. Let $a \neq b$. The following are equivalent.
i. $f^{-1}(a) \cap g^{-1}(b) = \emptyset$.
ii. $J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_1) = \emptyset$ and $J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_1)$ have cardinality $|D|$.
iii. (Mimics) There exists a bijection G such that $J_3(f,g,a,b)_1 = F_5G \wedge J_3(f,g,a,b)_2 = F_6G$.

Proof: i $\leftrightarrow$ ii is by Lemma 3.2.14. Assume ii. D is partitioned into the three sets $J_3(f,g,a,b)_1{}^{-1}(a_0) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_0)$, $J_3(f,g,a,b)_1{}^{-1}(a_1) \cap J_3(f,g,a,b)_2{}^{-1}(a_1)$ of cardinality $|D|$. D is also partitioned into the three sets $F_5{}^{-1}(a_0) \cap F_6{}^{-1}(a_0)$, $F_5{}^{-1}(a_1) \cap F_6{}^{-1}(a_0)$, $F_5{}^{-1}(a_1) \cap F_6{}^{-1}(a_1)$ of cardinality $|D|$ as they are $rng(h_2),rng(h_3),rng(h_4)$. Take G to be a bijection from each of the former three sets to the latter three sets. This establishes ii → iii. Now suppose G is a bijection with $J_3(f,g,a,b)_1 = F_5G$ ∧ $J_3(f,g,a,b)_2 = F_6G$. Now the three sets associated with $J_3(f,g,a,b)_1,J_3(f,g,a,b)_2$ are the inverse images under G of the three sets associated with F_5,F_6 in this way. All fix of these sets have cardinality |D|. QED

LEMMA 3.2.16. $a \neq b \wedge f^{-1}(a) \cap g^{-1}(b) \neq \emptyset$ is A*-bool/LUF/fmst in free variables f,g,a,b with the 14 active parameters, where the definition is correct in all alternative parameters.

Proof: The following holds.
1. $a \neq b \wedge f^{-1}(a) \cap g^{-1}(b) \neq \emptyset \leftrightarrow$
2. $a \neq b \wedge \neg(\exists G)(G$ is a bijection $\wedge J_3(f,g,a,b)_1 = F_5G \wedge J_3(f,g,a,b)_2 = F_6G) \leftrightarrow$
3. $a \neq b \wedge (\forall f',g')(J_3(f,g,a,b) = (f',g') \rightarrow \neg(\exists G)(G$ is a bijection $\wedge f' = F_5G \wedge g' = F_6G))$

To see 1 ↔ 2, assume a ≠ b, and note that $f^{-1}(a) \cap g^{-1}(b) = \emptyset$ is equivalent to Lemma 3.2.15iii, which is equivalent to saying that F5,F6 mimics $J_3(f,g,a,b)_1,J_3(f,g,a,b)_2$. I.e., these two pairs of functions are related by a bijection G of the domain D. 2 ↔ 3 is by a quantifier manipulation. By Lemma 3.2.14, $J_3(f,g,a,b)_1 = f' \wedge J_3(f,g,a,b)_2 = g'$ is E*-bool/LUF in the 14 active parameters and "G is a bijection" is E*-bool/LUF in the active parameter id by Lemma 3.2.7vii. QED

LEMMA 3.2.17. $(\forall x,y)(x \neq y \rightarrow (\exists!z)(f(z) = x \wedge g(z) = y))$ is A*-bool/LUF/fmst in free variables f,g with the 14 active parameters, where the definition is correct in all alternative parameters.

Proof: We have the following.
1. $(\forall x,y)(x \neq y \rightarrow (\exists!z)(f(z) = x \wedge g(z) = y)) \leftrightarrow$
2. $(\forall x,y)(x \neq y \rightarrow (\exists$ at most one $z)(f(z) = x \wedge g(z) = y)) \wedge (\forall x,y)(x \neq y \rightarrow (\exists z)(f(z) = x \wedge g(z) = y)) \leftrightarrow$
3. $(\forall x,y)(x \neq y \rightarrow (\exists$ at most one $z)(f(z) = x \wedge g(z) = y)) \wedge (\forall x,y)(x \neq y \rightarrow f^{-1}(x) \cap g^{-1}(y) \neq \emptyset)$

By Lemma 3.2.16, 3 is A*-bool/LUF/fmst in free variables f,g with the 14 active parameters, where the definition is correct in all alternative parameters. QED

LEMMA 3.2.18. $(\forall x)(\exists!z)(f(z) = x \wedge g(z) = x)$ is the conjunction of A*-bool/LUF/fmst and E*-bool/LUF/fmst in free variables f,g and active parameter id.

Proof: We have the following.
1. $(\forall x)(\exists!z)(f(z) = x \wedge g(z) = x) \leftrightarrow$
2. $(\forall x)(\exists$ at most one $z)(f(z) = x \wedge g(z) = x) \wedge (\forall x)(\exists z)(f(z) = x \wedge g(z) = x) \leftrightarrow$
3. $(\forall x)(\exists$ at most one $z)(f(z) = x \wedge g(z) = x) \wedge (\exists h)(\forall x)(f(h(x)) = x \wedge g(h(x)) = x) \leftrightarrow$
4. $(\forall x)(\exists$ at most one $z)(f(z) = x \wedge g(z) = x) \wedge (\exists h)((\forall x)(f(h(x)) = x) \wedge (\forall x)(g(h(x)) = x)) \leftrightarrow$
5. $(\forall x)(\exists$ at most one $z)(f(z) = x \wedge g(z) = x) \wedge (\exists h)(fh = id \wedge gh = id)$

QED

DEFINITION 3.2.12. A pairing pair consists of f,g where $(\forall x,y)(\exists!z)(f(z) = x \wedge g(z) = y)$.

LEMMA 3.2.19. "f,g is a pairing pair" is the conjunction of E*-bool/LUF/fmst and A*-bool/LUF/fmst in free variables f,g and the 14 active parameters, where the definition is correct in all alternative parameters.

Proof: Since f,g is a pairing pair if and only if $(\forall x,y)(x \neq y \rightarrow (\exists!z)(f(z) = x \wedge g(z) = y) \wedge (\forall x)(\exists z)(f(z) = x \wedge g(z) = z)$, this is immediate from Lemmas 3.2.17 and 3.2.18. QED

LEMMA 3.2.20. There exists a pairing pair.

Proof: Let $G:D \rightarrow D^2$ be a bijection. Let $f(x) = G(x)_1 \wedge g(x) = G(x)_2$. Then $(\forall x,y)(\exists!z)(f(z) = x \wedge g(z) = y)$ by taking $z = G^{-1}(x,y)$. Also if $f(z) = f(w)$ and $g(z) = g(w)$ then $G(z)_1 = G(w)_1$ and $G(z)_2 = G(w)_2$. Hence $G(z) = G(w)$ and therefore $z = w$ (G is one-one). Hence f,g is a pairing pair. QED

DEFINITION 3.2.13. We fix a pairing pair P_1,P_2. We will later add it to an updated list of active parameters. For the time being, we use them for further constructions.

DEFINITION 3.2.14. We define $<x,y>P$ to be the unique z such that $P_1(z) = x \wedge P_2(z) = y$. We inductively define $<x_1,\ldots,x_n>P = <x_1,<x_2,\ldots,x_n>P>P$, $n \geq 3$. For $n \geq 2$, an n-system consists of functions $F[1,n],\ldots,F[n,n] \in DD$, where $(\forall x_1,\ldots,x_n)(\exists! y)(\forall i \leq n)(F[i,n](y) = x_i)$.

Here we use the letter P to reference that Definition 3.2.14 is relative to a choice of pairing pairs. Thus we view P as referring to the pairing pair P_1,P_2.

LEMMA 3.2.21. $<x,y>P$ is a bijection from D^2 onto D. $<x_1,\ldots,x_n>P$ is a bijection from D^n onto D. This holds for any pairing pair P_1,P_2.

Proof: Suppose $<x,y>P = <z,w>P$. Then $P_1(<x,y>P) = x = P_1(<z,w>P) = z$ and $P_2(<x,y>P) = y = P_2(<z,w>P) = w$. Let $z \in D$. We claim that $<P_1(z),P_2(z)>P = z$. For $<P_1(z),P_2(z)>P$ is the unique w such that $P_1(w) = P_1(z) \wedge P_2(w) = P_2(z)$. But z is one of these w's. Therefore $w = z$.

We prove the second claim by induction on $n \geq 2$. Let $n \geq 2$ and $<x_1,\ldots,x_n>P$ be a bijection from D^n onto D. Now $<x_1,\ldots,x_{n+1}>P = <x_1,<x_2,\ldots,x_n>P>P$. Let $y \in D$. Let y be such that $x_1 = P_1(y)$ and $<x_2,\ldots,x_n>P = P_2(y)$, which we can do since P_1,P_2 is a pairing pair. Hence $<x_1,\ldots,x_{n+1}>P = <x_1,<x_2,\ldots,x_n>P>P = y$. Now suppose $<x_1,\ldots,x_{n+1}>P = <y_1,\ldots,y_{n+1}>P = <x_1,<x_2,\ldots,x_{n+1}>P>P = <y_1,<y_2,\ldots,y_{n+1}>P>P$. Then $x_1 = y_1 \wedge <x_2,\ldots,x_{n+1}>P = <y_2,\ldots,y_{n+1}>P$, and so by induction hypothesis, $x_1,\ldots,x_{n+1} = y_1,\ldots,y_{n+1}$. QED

LEMMA 3.2.22. Let $n \geq 2$ and $x_1,\ldots,x_n \in D$. For all $1 \leq i \leq n-1$, $x_i = P_1P_2^{i-1}(<x_1,\ldots,x_n>P)$. $x_n = P_2^{n-1}(<x_1,\ldots,x_n>P)$.

Proof: We prove this by induction on $n \geq 2$. For $n = 2$, $x_1 = P_1P_2^0(<x_1,x_2>P) = P_1(<x_1,x_2>P) \wedge x_2 = P_2(<x_1,x_2>P)$ is immediate. Now suppose this is true for fixed $n \geq 2$. We have

1) Let $x_1,\ldots,x_n \in D$. For all $1 \leq i \leq n-1$, $x_i = P_1P_2^{i-1}(<x_1,\ldots,x_n>P) \wedge x_n = P_2^{n-1}(<x_1,\ldots,x_n>P)$

and want

2) Let $x_1,\ldots,x_{n+1} \in D$. For all $1 \leq i \leq n$, $x_i = P_1P_2^{i-1}(<x_1,\ldots,x_{n+1}>P) \wedge x_{n+1} = P_2^{n}(<x_1,\ldots,x_{n+1}>P)$

Now $\langle x_1,...,x_{n+1}\rangle P = \langle x_1,\langle x_2,...,x_{n+1}\rangle P\rangle P$, and so we apply 1) to $\langle x_2,...,x_{n+1}\rangle P$. Thus we have

3) For all $1 \leq i \leq n-1$, $x_{i+1} = P_1P_2^{i-1}(\langle x_2,...,x_{n+1}\rangle P) \wedge x_{n+1} = P_2^{n-1}(\langle x_2,...,x_{n+1}\rangle P)$

4) For all $1 \leq i \leq n-1$, $x_{i+1} = P_1P_2^{i}(\langle x_1,\langle x_2,...,x_{n+1}\rangle P\rangle P) \wedge x_{n+1} = P_2^{n}(\langle x_1,\langle x_2,...,x_{n+1}\rangle P\rangle P)$

5) For all $2 \leq i \leq n$, $x_i = P_1P_2^{i-1}(\langle x_1,...,x_{n+1}\rangle P) \wedge x_{n+1} = P_2^{n}(\langle x_1,\langle x_2,...,x_{n+1}\rangle P\rangle P)$

6) For all $1 \leq i \leq n$, $x_i = P_1P_2^{i-1}(\langle x_1,...,x_{n+1}\rangle P) \wedge x_{n+1} = P_2^{n}(\langle x_1,\langle x_2,...,x_{n+1}\rangle P\rangle P)$

which is the same as 2). QED

LEMMA 3.2.23. For all $n \geq 2$, the n functions $P_1P_2^{i-1}, P_2^{n-1}$, $1 \leq i \leq n-1$, form an n-system.

Proof: Let $n \geq 2$ and $x_1,...,x_n \in D$. Then the n functions $P_1P_2^{i-1}, P_2^{n-1}, P_2^{n-1}$ at $\langle x_1,...,x_n\rangle$ are $x_1,...,x_n$, respectively, and so we have existence in the definition of n-system setting $z = \langle x_1,...,x_n\rangle$.

For uniqueness, suppose the n functions $P_1P_2^{i-1}, P_2^{n-1}, P_2^{n-1}$ at z and at w are $x_1,...,x_n$. We claim $z = \langle x_1,...,x_n\rangle$. To see this, by Lemma 3.2.21, let $z = \langle x_1',...,x_n'\rangle$. By Lemma 3.2.22, the n functions $P_1P_2^{i-1}, P_2^{n-1}, P_2^{n-1}$ at $\langle x_1',...,x_n'\rangle P$ are $x_1',...,x_n'$, respectively. Since $z = \langle x_1',...,x_n'\rangle$, the n functions $P_1P_2^{i-1}, P_2^{n-1}, P_2^{n-1}$ at z are $x_1',...,x_n'$, respectively. Hence $x_1,...,x_n = x_1',...,x_n'$. So $z = \langle x_1,...,x_n\rangle P$. Similarly, for w, we have $w = \langle x_1,...,x_n\rangle P$. By Lemma 3.2.21, $z = w$. QED

DEFINITION 3.2.15. We define $P[i,n]$, $n \geq 2$, $1 \leq i \leq n-1$, by $P[i,n] = P_1P_2^{i-1}$, $P[n,n] = P_2^{n-1}$.

LEMMA 3.2.24. For all $n \geq 2$, $P[1,n],...,P[n,n]$ is an n-system. $P[1,n](\langle x_1,...,x_n\rangle P) = x_1 \wedge ... \wedge P[n,n](\langle x_1,...,x_n\rangle P) = x_n$.

Proof: Immediate from Lemmas 3.2.22 and 3.2.23. QED

DEFINITION 3.2.16. φ is n-special if and only if for some (unique) $n \geq 1$, φ is a propositional combination of equations v1 = v2,...,v2n-1 = v2n. There is no problem requiring that all of these equations must appear in φ in order for φ to be n-special. We define functions $P_\varphi \in DD$, where φ is n-special, as follows.
$(\forall y)(\varphi(P[1,2n](y)=P[2,2n](y),...,P[2n-1,2n](y)=P[2n,2n](y)) \leftrightarrow P_\varphi(y) = y)$. Obviously P_φ is not unique, so we fix one such P_φ for each n-special φ, arbitrarily. φ is special if and only if φ is n-special for some $n \geq 1$.

DEFINITION 3.2.17. We now extend our list of active parameters and parameter requirements. Note that all of these parameter requirements lie in the language LUF.
$h_1,h_2,h_3,h_4,H,a_0,a_1,F_1,F_2,F_3,F_4,F_5,F_6,id,d^*,P_1,P_2,P[i,n],P_\varphi$ with the following parameter requirements.
i. $a_0 \neq a_1$ from D.
ii. $R(h_1,h_2,h_3,h_4,H)$.
iii. $F_1(a_0) = a_0 \wedge (\forall x)(x \neq a_0 \rightarrow F_3(x) = a_1)$.
iv. $F_2(a_1) = a_0 \wedge (\forall x)(x \neq a_1 \rightarrow F_4(x) = a_0)$.
v. F_3 is the identity on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_1 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
vi. F_4 is the identity on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_0 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
vii. F_5 is constantly a_0 on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_1 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
viii. F_6 is constantly a_0 on $rng(h_1)$, constantly a_0 on $rng(h_2)$, constantly a_0 on $rng(h_3)$, constantly a_1 on $rng(h_4)$.
ix. id is a (the) identity function.
x. d* is a constant function.
xi. P_1,P_2 is a pairing pair using the definition in Lemma 3.2.19 involving i-ix.
xii. $P[i,n]$, $1 \leq i \leq n$, $n \geq 2$, using Definition 3.2.15 involving P_1,P_2.
xiii. P_φ, φ special, using Definition 3.2.16 involving xii.

LEMMA 3.2.25. The parameter requirement is an infinite list of formulas from E*-bool/LUP/fm and A*-bool/LUP/fm. The values of these active parameters under j_0,j_1 form alternative parameters.

Proof: First claim evident by inspection. Lots of connectives arise in xiii. The use of E*-bool/LUP/fm arises with xi (although it can be eliminated). The second claim is from j0,j1 being E*-bool/LUF preserving. QED

LEMMA 3.2.26. Let φ be n-special. $(\forall x_1,\ldots,x_{2n})(\varphi(x_1,\ldots,x_{2n}) \leftrightarrow P_\varphi(<x_1,\ldots,x_{2n}>P) = <x_1,\ldots,x_{2n}>P)$.

Proof: From Definition 3.2.16, we have $(\forall y)(\varphi(P[1,2n](y)=P[2,2n](y),\ldots,P[2n-1,2n](y)=P[2n,2n](y)) \leftrightarrow P_\varphi(y) = y)$. Set $y = <x_1,\ldots,x_{2n}>P$. QED

We now expand LUF to the language of multivariate functions, LMF. This is our third language and we will use one more later. We still work with only one model based on D, but with infinitely many sorts beginning with D,DD. The terms will always have values in D, which was not the case with LUF, where we had terms of both sorts D and DD.

DEFINITION 3.2.18. FCN(n,D) is the set of all n-ary functions from D into D. We use FCN(1,D) interchangeably with DD. LMF (language of multivariate functions) is the language with the infinitely many sorts D,FCN(1,D),FCN(2,D),... . We use variables v_i, $i \geq 1$, over D, and function variables $f^n{}_i$ over FCN(n,D). We will only work with the specific LMF structure M = (D,FCN(1,D),FCN(2,D)...), which carries the application functions A_n:FCN(n,D) × $D^n \rightarrow D$ given by $A_n(f^n{}_i,x_1,\ldots,x_n) = f^n{}_i(x_1,\ldots,x_n)$. We don't use • in LMF. We don't actually use these A's, as they are implicit in the way we handle terms. The terms are inductively defined as follows. The variables of sort D are terms. $f^n{}_i(t_1,\ldots,t_n)$ is a term if $t_1,\ldots,t_n$ are terms. The atomic formulas are of the form s = t, where s,t are terms. The formulas are generated by the atomic formulas by propositional connectives, and quantification over the sorts as usual.

Note that strictly speaking, LMF is not an extension of LUF, having removed • and also only allowing terms of sort D.

DEFINITION 3.2.19. We distinguish between formulas, statements, and formula statements in LMF the same way that we did in LUF in Definition 3.2.5. We continue to use a,b,c,d,u,v,w,x,y,z, with and without subscripts and ', for elements of D, unless indicated otherwise. We use f,g,h, with and without subscripts and ', for elements of DD, unless indicated otherwise. We use F,G,H, with and without subscripts and ' for elements of the FCN(n,D), n ≥ 2 and various, unless indicated otherwise. We often leave off the numerical superscript that indicates the arity.

The use of lower case f,g,h for unary functions and upper case F,G,H for functions of arity ≥2 is expositionally convenient.

DEFINITION 3.2.20. 1st/LMF/fm, 1st/LMF/st, 1st/LMF/fmst is the set of all formulas, statements, formula statements where all quantifiers range over D. A*1st/LMF/fm, A*1st/st, A*1st/fmst is the set of all formulas, statements, formula statements beginning with zero or more universal quantifiers ranging over any sorts, followed by a formula, statement, or formula statement whose quantifiers range over D. E*1st/LUF/fm, E*1st/LUF/st, E*1st/LUF/fmst are the same with "universal" replaced by "existential". A formula statement is basic if and only if every equation in the formula has at most one occurrence of a function variable, and this one occurrence occurs on the left.

DEFINITION 3.2.21. We will eventually extend j_0,j_1 to the list $j_0,j_1,j_2,...$, where $j_i:D^i \rightarrow D$, $i \geq 0$. $j_0,j_1,...$ is K/LUF preserving if and only if any element of K/LUF/st holds if and only if it holds with all parameters replaced by their values under $j_0,j_1,j_2,...$. Here K is any class of statements in LMF.

We now want to replace ≥2-ary functions with unary functions.

DEFINITION 3.2.22. Let $F:D^n \rightarrow D$, $n \geq 2$. UN(F,P) ∈ DD is given by UN(F,P)(x) = F(P[1,n](x),...,P[n,n](x)).

LEMMA 3.2.27. Let $n \geq 2$. $F(x_1,...,x_n) = UN(F,P)(<x_1,...,x_n>P)$. The operation that sends F ∈ FCN(n,D) to UN(F,P) is a bijection from FCN(n,D) onto DD. This holds for any alternative parameters.

Proof: By definition $UN(F,P)(<x_1,...,x_n>P) = F(P[1,n](<x_1,...,x_n>P,...,P[n,n](<x_1,...,x_n>P)) = F(x_1,...,x_n)$. For the second claim, let UN(F,P) = UN(G,P). Then $F(x_1,...,x_n) = UN(F,P)(<x_1,...,x_n>P) = UN(G,P)(<x_1,...,x_n>P) = G(x_1,...,x_n)$, and hence F = G. For surjectively, let f ∈ DD. Let $F(x_1,...,x_n) = f(<x_1,...,x_n>P)$. Then $F(x_1,...,x_n) = UN(F,P)(<x_1,...,x_n>P)$ and so f and UN(F,P) agree at all $<x_1,...,x_n>P$. But by Lemma 3.2.21, these $<x_1,...,x_n>P$ are all the elements of D, and hence f = UN(F,P). QED

LEMMA 3.2.28. (Elimination of arity ≥2). Let φ be a quantifier free formula in LMF with variables $x_1,...,x_n,f_1,...,f_m,G_1,...,G_r$. There exists basic φ' in E*=/LUF/fmst with free variables $x_1,...,x_n,f_1,..,f_m,g_1,...,g_r$ and all parameters active, such that $(\forall x_1,...,x_n)(\forall f_1,...,f_m)(\forall g_1,...,g_r)(\forall G_1,...,G_r)(UN(G_1,P) = g_1 \wedge ... \wedge UN(G_r,P) = g_r \rightarrow (\varphi \leftrightarrow \varphi'))$. This holds for any alternative parameters.

Proof: φ is a propositional combination α of equations in LMF, $\alpha(s_1=t_1,...,s_k=t_k)$, where α is k-special. Hence φ is equivalent to $P_\alpha(<s_1,t_1,...s_k,t_k>) = <s_1,t_1,...,s_k,t_k>$ and therefore to $(\exists y)(P_\alpha(y) = y \wedge P[1,2k](y) = s_1 \wedge P[2,2k](y) = t_1 \wedge ... \wedge P[2k-1,2k](y) = s_k \wedge P[2k,2k](y) = t_k)$. Now the s_i,t_i may not be basic, but we can introduce existential quantifiers to unravel them in the usual way to come to $(\exists y,z_1,...,z_t)(\psi)$, where ψ is a finite conjunction of basic equations. The ones with a ≥2 ary function variable are $G_{i1}(u_1,...,u_p) = v,...,G_{ib}(u_1,...,u_p) = v$, where u's,p's,v's are various. The basic ψ' results from ψ by replacing each $G_{ij}(u_1,...,u_p) = v$ by $g_{ij}(<u_1,...,u_p>) = v$, and then by $g_{ij}(w_j) = v \wedge P[1,p](w_j) = u_1 \wedge ... \wedge P[p,p](w_j) = u_p$, preparing to existentially quantify out the w's. So we take basic φ' = $(\exists y,z_1,...,z_t,w_1,...,w_b)(\psi')$ with free variables $x_1,...,x_n,f_1,...,f_m,g_1,...,g_r$ and all parameters active. All manipulations are universally correct until we replace the $G_{ij}(u_1,...,u_p) = v$ by $g_{ij}(w_j) = v \wedge P[1,p](w_j) = u_1 \wedge ... \wedge P[p,p](w_j) = u_p$ with w_j existentially quantified out. But assume $UN(G_1,P) = g_1 \wedge ... \wedge UN(G_r,P) = g_n$. Then those existentially quantified out replacements are universally correct. QED

LEMMA 3.2.29. (Arity ≥2 Skolem Functions). Let φ = $(\exists F_1,...,F_k)(\psi)$ be an E*1st/LMF/fm with free variables $x_1,...,x_n,f_1,...,f_m,G_1,...,G_r$. There exists E*1st/LMF/fm, φ' = $(\exists F_1,...,F_{k+s})(\forall y1,...,y_s)(\psi')$, with the same free variables, where ψ' is quantifier free, such that $(\forall x_1,...,x_n)(\forall f_1,...,f_m)(\forall G_1,...,G_r)(\varphi \leftrightarrow \varphi')$.

Proof: Put φ in prenex normal form φ_1 = $(\exists F_1,\ldots,F_k)(\forall y_1)(\exists z_1)\ldots(\forall y_s)(\exists z_s)(\psi_1)$, ψ_1 quantifier free, where the quantified variables are distinct and distinct from the free variables of φ. Some of these quantifiers may be dummy, but that does not cause any difficulties. Now use the standard Skolem function construction. In ψ_1, replace each occurrence of z_i by $F_{k+i}(y_1,\ldots,y_i)$, $1 \leq i \leq s$. A minor issue is that F_{k+1} is unary here, and so we can't use capital F. So we replace z_1 by $F_{k+1}(y_1,y_1)$ instead of the 'illegal' $F_{k+1}(y_1)$. We have φ is equivalent to φ' = $(\exists F_1,\ldots,F_{k+s})(\forall y_1,\ldots,y_k)(\psi')$, universally. QED

LEMMA 3.2.30. (Elimination of arity ≥2 applied). Let φ = $(\exists F_1,\ldots,F_k)(\forall y_1,\ldots,y_s)(\psi) \in$ E*1st/LMF/fm, with free variables $x_1,\ldots,x_n,f_1,\ldots,f_m,G_1,\ldots,G_r$, where ψ is quantifier free. There exists φ' = $(\exists h_1,\ldots,h_k)(\forall y_1,\ldots,y_s)(\exists z_1,\ldots,z_t)(\psi') \in$ LUF/fmst, ψ' a finite conjunction of equations, with free variables $x_1,\ldots,x_n,f_1,\ldots,f_m,g_1,\ldots,g_r$, and active parameters, such that $(\forall x_1,\ldots,x_n)(\forall f_1,\ldots,f_m)(\forall g_1,\ldots,g_r)(\forall G_1,\ldots,G_r)(g_1 = \mathrm{UN}(G_1,P) \wedge \ldots \wedge g_n = \mathrm{UN}(G_n,P) \rightarrow (\varphi \leftrightarrow \varphi'))$. This holds for any alternative parameters.

Proof: ψ has free variables $x_1,\ldots,x_n,f_1,\ldots,f_m,G_1,\ldots,G_r,F_1,\ldots,F_k$. First apply Lemma 3.2.28 to put ψ in the form $(\exists z_1,\ldots,z_t)(\psi')$ in E*=/LUF/fmst, with free variables $x_1,\ldots,x_n,f_1,\ldots,f_m,g_1,\ldots,g_r,h_1,\ldots,h_k$ and active parameters, such that $x_1,\ldots,x_n,f_1,\ldots,f_m,g_1,\ldots,g_r$, such that $(\forall x_1,\ldots,x_n)(\forall f_1,\ldots,f_m)(\forall g_1,\ldots,g_r)(\forall G_1,\ldots,G_r)(\forall F_1,\ldots,F_k)(\mathrm{UN}(G_1,P) = g_1 \wedge \ldots \wedge \mathrm{UN}(G_r,P) = g_r \wedge \mathrm{UN}(F_1,P) = h_1 \wedge \ldots \wedge \mathrm{UN}(F_k,P) = h_k \rightarrow (\psi \leftrightarrow \psi'))$. Now let φ' = $(\exists h_1,\ldots,h_k)(\forall y_1,\ldots,y_s)(\exists z_1,\ldots,z_t)(\psi')$.

Let $x_1,\ldots,x_n,f_1,\ldots,f_m,g_1,\ldots,g_r,G_1,\ldots,G_r$ be given, where $g_1 = \mathrm{UN}(G_1,P) \wedge \ldots \wedge g_n = \mathrm{UN}(G_n,P)$. Assume φ = $(\exists F_1,\ldots,F_k)(\forall y_1,\ldots,y_s)(\psi)$. Fix $F_1,\ldots,F_k$ such that $(\forall y_1,\ldots,y_s)(\psi)$. Let $y_1,\ldots,y_s$ be given. Let h_1 = $\mathrm{UN}(F_1,P),\ldots,h_k = \mathrm{UN}(F_k,P)$. By Lemma 3.2.28, ψ' holds. Hence $(\forall y_1,\ldots,y_s)(\psi')$. Hence $(\exists h_1,\ldots,h_k)(\forall y_1,\ldots,y_s)(\psi') = \varphi'$. Conversely, assume $\varphi' = (\exists h_1,\ldots,h_k)(\forall y_1,\ldots,y_s)(\psi')$. Let $h_1,\ldots,h_k$ be such that $(\forall y_1,\ldots,y_s)(\psi')$. By Lemma 3.2.27, let $\mathrm{UN}(F_1,P) = h_1,\ldots,\mathrm{UN}(F_k,P) = h_k$. Let $y_1,\ldots,y_s$ be given.

By Lemma 3.2.28, ψ holds. Hence $(\forall y_1,...,y_s)(\psi)$ holds. Therefore $(\exists F_1,...,F_k)(\forall y_1,...,y_s)(\psi) = \varphi$ holds. QED

LEMMA 3.2.31. Let $\varphi = (\exists h_1,...,h_k)(\forall y_1,...,y_s)(\exists z_1,...,z_t)(\psi) \in$ LUF/fmst, ψ a finite conjunction of equations, with free variables $x_1,...,x_n,f_1,...,f_m$, and active parameters. There exists $\varphi' = (\exists h_1,...,h_{k+t})(\forall y)(\psi')$ with free variables $x_1,...,x_n,f_1,...,f_m$, and active parameters, ψ' a finite conjunction of equations, such that $(\forall x_1,...,x_n)(\forall f_1,...,f_m)(\varphi \leftrightarrow \varphi')$. This holds for any alternate parameters.

Proof: φ is equivalent to $(\exists h_1,...,h_k)(\forall y)(\exists z_1,...,z_t)(\psi_0)$, where ψ_0 is obtained from ψ by replacing each y_i by P[1,s](y). We now introduce $h_{k+1},...,h_{k+t}$ for t unary Skolem functions, and take ψ' to result from ψ_0 by replacing each z_i by $h_{k+i}(y)$. Obviously we have equivalence with $(\exists h_1,...,h_{k+t})(\forall y)\psi') = \varphi'$. QED

LEMMA 3.2.32. Every formula $(\forall y)(s = t)$ in LUF is equivalent to an E*-bool/LUFfmst with the same free variables, using the active parameter d*. This holds for any alternate parameters.

Proof: If s,t do not mention y then $(\forall y)(s = t)$ is equivalent to s = t. If s,t both mention y then we have $(\forall y)(s'y = t'y)$ which is equivalent to s' = t'. Suppose s mentions y and t does not. If s is just y then $(\forall y)(y = t)$ is equivalent to $t \neq t$. Otherwise, we have

$(\forall y)(s'y = t) \leftrightarrow$

$s' \in C \wedge (\exists y)(s'y = t) \leftrightarrow$

$(\exists g)(s' = gd^*) \wedge (\exists y)(s'y = t)$

$(\exists g,y)(s' = gd^* \wedge s'y = t)$

using the active parameter d* and Lemma 3.2.7iv. QED

LEMMA 3.2.33. Let $\varphi \in$ E*1st/LMF/fm with free variables $x_1,...,x_n,f_1,...,f_m,G_1,...,G_r$. There exists $\gamma \in$ E*-bool/LUF/fmst with free variables $x_1,...,x_n,f_1,...,f_m,g_1,...,g_r$, and active parameters, such that $(\forall x_1,...,x_n)(\forall f_1,...,f_m)(\forall g_1,...,g_r)(\forall G_1,...,G_r)(g_1 = \mathrm{UN}(G_1,P) \wedge ... \wedge g_r = \mathrm{UN}(G_r,P) \rightarrow (\varphi \leftrightarrow \gamma))$. This holds for any alternative parameters.

Proof: Let $\varphi, x_1, ..., x_a, h_1, ..., h_b, G_1, ..., G_n$ be as given. Write $\varphi = (\exists F_1, ..., F_k)(\psi)$. The outermost (existential) quantifiers of φ may have some quantifiers over D and some quantifiers over DD, and these quantifiers can be moved in so that all of the outermost existential quantifiers are of arity ≥2 and we can use capital letters. So write $\varphi = (\exists F_1, ..., F_k)(\psi)$ as in Lemma 3.2.27. So using Lemmas 3.2.28 - 3.2.32 we have the following chain of universal equivalences under the hypothesis g1 = UN(G1,P) ∧ ... ∧ gn = UN(Gn,P).

1. $(\exists F_1, ..., F_k)(\psi) \leftrightarrow$
2. $(\exists F_1, ..., F_{k1})(\forall y_1, ..., y_s)(\psi_1) \leftrightarrow$
3. $(\exists h_1, ..., h_{k2})(\forall y_1, ..., y_s)(\exists z_1, ..., z_t)(\psi_2) \leftrightarrow$
4. $(\exists h_1, ..., h_{k3})(\forall y)(\psi_3) \leftrightarrow$
5. $(\exists h_1, ..., h_{k4})((\forall y)(\alpha_1) \wedge ... \wedge (\forall y)(\alpha_c)) \leftrightarrow$
6. $(\exists h_1, ..., h_{k4})(\beta_1 \wedge ... \wedge \beta_c) \leftrightarrow$
7. γ

1 ↔ 2 by Lemma 3.2.29.
2 ↔ 3 by Lemma 3.2.30.
3 ↔ 4 by Lemma 3.2.31.
4 ↔ 5 by logic.
5 ↔ 6 by Lemma 3.2.32.
6 ↔ 7 by logic.

1,2 are in LMF and 3-7 are in LUF. We need the hypothesis $g_1 = UN(G_1,P) \wedge ... \wedge g_n = UN(G_n,P)$ for 2 ↔ 3 only.

ψ, ψ_1 are quantifier free. ψ_2, ψ_3 are finite conjunctions of equations. $\alpha_1, ..., \alpha_c$ are equations. $\beta_1, ..., \beta_c$ are in E*=/LUF/fmst. γ in E*-bool/LUF/fmst.

The free variables of 1,2 are $x_1, ..., x_n, f_1, ..., f_m, G_1, ..., G_r$.
The free variables of 2-7 are $x_1, ..., x_n, f_1, ..., f_m, h_1, ..., h_r$.

There are no parameters in 1,2. All parameters in 3-7 are active parameters.

$\beta_1, ..., \beta_c$ are in E*=/LUF. γ is in E*-bool/LUF/fmst.

All of these equivalences hold for any alternative parameters. QED

DEFINITION 3.2.23. For $n \geq 2$, we define j_n:FCN(n,D) → FCN(n,D) as follows. $j_n(F) \in$ FCN(n,D) is unique such that UN(j_n(F),P) = j_1(UN(F,P)).

LEMMA 3.2.34. j_0,j_1 of the active parameters collectively form alternative parameters. j_n:FCN(n,D) → FCN(n,D) is uniquely defined by Definition 3.2.24.

Proof: The parameter requirements are in A*-bool/LUP/fm or E*-bool/LUP/fm and therefore preserved under j_0,j_1. This establishes the first claim. By Lemma 3.2.27, the operation that sends G to UN(G,P) is a bijection from FCN(n,D) onto DD. It follows immediately that for any F ∈ FCN(n,D), there is a unique G ∈ FCN(n,D) with UN(G,P) = j_1(UN(F,P)). Thus j_n(F) = G is well defined. QED

If we use alternative parameers P' then Lemma 3.2.33 still holds but we would get a different j_n, $n \geq 2$.

LEMMA 3.2.35. $j_0,j_1,j_2,\ldots$ is E*1st/LMF preserving from (D,FCN(1,D),FDN(2,D),...) into (D,FCN(1,D),FCN(2,D),...).

Proof: Let φ ∈ E*1st/LMF/st with free variables $x_1,\ldots,x_n,f_1,\ldots,f_m,G_1,\ldots,G_r$. Let γ ∈ E*-bool/LUF/fmst be given by Lemma 3.2.33. γ has free variables $x_1,\ldots,x_n$,f1,...,f_m,g1,...,g_r and also active parameters. Then we have

1. φ holds at $x_1,\ldots,x_n,f_1,\ldots,f_m,G_1,\ldots,G_r$ ↔
2. γ holds at $x_1,\ldots,x_n,f_1,\ldots,f_m$,UN($G_1$,P),...,UN($G_r$,P) ↔
3. γ holds at $j_0(x_1),\ldots,j_0(x_n),j_1(f_1),\ldots,j_1(f_m)$,$j_1$(UN($G_1$,P),...,$j_1$(UN($G_r$,P)) ↔
4. γ holds at $j_0(x_1),\ldots,j_0(x_n),j_1(f_1),\ldots,j_1(f_m)$,j($G_1$,P),...,j($G_r$,P)) ↔
5. φ holds at $j_0(x_1),\ldots,j_0(x_n),j_1(f_1),\ldots,j_1(f_m)$,j($G_1$,P),...,j($G_r$,P)).

1 ↔ 2 is by Lemma 3.2.33. 2 ↔ 3 is by j_0,j_1 being E*-bool/LUF preserving. However bear in mind that there are generally active parameters in 2 and we must use their values under j_0,j_1 in 3. 3 ↔ 4 is by Definition 3.2.23. 4 ↔ 5 is by Lemma 3.2.33, however there is a major point here. We are not using the active parameters that were used for

getting 1 ↔ 2 from Lemma 3.2.33. Instead we are using the j_0,j_1 values of the active parameters. However they form alternative parameters by Lemma 3.2.25. So according to Lemma 3.2.33, the equivalence there works is we use any alternative parameters. QED

Now that we have the very powerful Lemma 3.2.36, we have no need for keeping track of the active parameters, and we release them.

We now extend LMF to the larger language LMFR = language of multivariate functions and relations.

DEFINITION 3.2.24. REL(n,D) is the set of all n-ary relations on D; i.e., subsets of D^n, $n \geq 1$. LMFR (language of multivariate functions and relations) is the language with the infinitely many sorts S,FCN(1,D),FCN(2,D),...,REL(1,D),REL(2,D),... . We use variables v_i, $i \geq 1$, over D, function variables $f^n{}_i$ over FCN(n,D), and relation variables $R^n{}_i$ over REL(n,D). We will only work with the specific LMFR structure M = (D,FCN(1,D),...,REL(1,D),...), which carries the application functions A_n:FCN(n,D) × $D^n \rightarrow D$ given by $A_n(f^n{}_i,x_1,...,x_n) = f^n{}_i(x_1,...,x_n)$, and the application relations $T_n \subseteq$ REL(n,D) x S^n given by $T_n(R,x_1,...,x_n) \leftrightarrow R(x_1,...,x_n)$. We don't actually use these A's and T's. The terms are inductively defined as follows. The variables of sort D are terms. $f^n{}_i(t_1,...,t_n)$ is a term if $t_1,...,t_n$ are terms. The atomic formulas are of the form s = t and $R(t_1,...,t_n)$, where $s,t,t_1,...,t_n$ are terms and R is an n-ary relation variable. The formulas are generated by the atomic formulas by propositional connectives, and quantification over the sorts as usual. A*1st/LMFR, E*1st/LMFR are defined as in LMF where of course the outer quantifiers and the free variables and parameters can be of any sort including the new relation sorts.

We emphasize that as in LMF, all terms of LMFR are of sort D.

We now extend the j's.

DEFINITION 3.2.25. For F ∈ FCN(n,D), define rel(F) = $\{(x_1,...,x_n):F(x_1,...,x_n) = x_1\}$. We define j_n':REL(n,D) → REL(n,D) by j_n'(A) = rel(j_n(F)) where rel(F) = A.

Note that no parameters are used to define the j_n'.

LEMMA 3.2.36. Each j_n' is well defined. j'(rel(F)) = rel(j(F)). $j_0,...,j_1',...$ is E*1st/LMFR preserving.

Proof: For the first claim, we need that we can find F such that rel(F) = A. This is trivial. We also need unambiguity. Let rel(F) = rel(G) = R. We need to check that rel(j_n(F)) = rel(j_n(G)). I.e., $(\forall x_1,...,x_n)(j_n(F)(x_1,...,x_n) = x_1 \leftrightarrow j_n(G)(x_1,...,x_n))$. Since $(\forall x_1,...,x_n)(F(x_1,...,x_n) = x_1 \leftrightarrow G(x_1,...,x_n) = x_1)$, this follows by 1st/LFM preserving. For the second claim, j'(rel(F)) is rel(j(G)) for any G with rel(G) = rel(F). Use G = F.

For the third claim, let $(\exists x_1,...,x_n)(\exists f_1,...,f_m)(\exists F_1,...,F_r)(\exists R_1,...,R_s)(\varphi)$ be E*1st/LMFRst with parameters $y_1,...,y_a,g1,...,g_b,G_1,...,G_c,S_1,...,S_d$. For all $J_1,...,J_d$ with $rel(J_1) = S_1,...,rel(J_d) = S_d$,

1. $(\exists x_1,...,x_n)(\exists f_1,...,f_m)(\exists F_1,...,F_r)(\exists R_1,...,R_s)(\varphi) \leftrightarrow$
2. $(\exists x_1,...,x_n)(\exists f_1,...,f_m)(\exists F_1,...,F_r)(\exists H_1,...,H_s)(\psi) \leftrightarrow$
3. $(\exists x_1,...,x_n)(\exists f_1,...,f_m)(\exists F_1,...,F_r)(\exists H_1,...,H_s)(\rho) \leftrightarrow$
4. $(\exists x_1,...,x_n)(\exists f_1,...,f_m)(\exists F_1,...,F_r)(\exists R_1,...,R_s)(\sigma)$

where

a. $\psi = \varphi[R_i(t_1,...,t_p)/H_i(t_1,...,t_p)=t_1;S_i(t_1,...,t_p)/J_i(t_1,...,t)=t)$.
b. $\rho = \psi[y_i,g_i,G_i,J_i/j_0(y_i),j_1(g_i),j(G_i),j(J_i)]$
c. $\sigma = \rho[j(J_i)(t_1,...,t_p)=t_1/rel(j(J_i))(t_1,...,t_p);H_i(t_1,...,t_p)=t_1/R_i(t_1,...,t_p)]$
d. $\sigma = \rho[j(J_i)(t_1,...,t_p)=t_1/j'(rel(J_i))(t_1,...,t_p);H_i(t_1,...,t_p)=t_1/R_i(t_1,...,t_p)]$
e. $\sigma = \rho[j(J_i)(t_1,...,t_p)=t_1/j'(S_i)(t_1,...,t_p);H_i(t_1,...,t_p)=t_1/R_i(t_1,...,t_p)]$
f. $\sigma = \varphi[y_i,g_i,G_i,S_i/j_0(y_i),j_1(g_i),j(G_i);j'(S_i)]$

1 $\leftrightarrow$ 2 via 'a' is by definition of rel operator, from R's we go to H's and from H's we go to R's. Eliminates relations in favor of functions.

2 ↔ 3 is by $j_0, j_1, ...$ being E*1st/LMF preserving, so application of j's to the parameters.
3 ↔ 4 puts the relations that were eliminated back to the original functions. c,d,e are based on $rel(j(J_i)) = j'(rel(J_i)) = j'(S_i)$, by second claim and the hypothesis.
3 ↔ 4 via f composes the replacement to take φ to ψ and from ψ to ρ and from ρ to α to a replacement that takes φ to σ.

1 ↔ 4 via f establishes the preserving for the third claim. QED

DEFINITION 3.2.26. We move our j's to a convenient set S of the same cardinality as D via an arbitrary bijection h:D → S. We choose our S as follows. Let α be the greatest ordinal such that $|V(\alpha)| \leq |D|$. Let $V(\alpha) \subseteq S \subseteq V(\alpha+1)$, where $|S| = |D|$. So we have $j_0*, ..., j_1'*, ...$ as in Lemma 3.2.36, this time on S,FCN(1,S),...,REL(1,S),... . We leave the *'s off and write $j_0, ..., j_1', ..,$ where $j_0:S \to S$, $j_n:FCN(n,S) \to FCN(n,S)$, $j_n':REL(n,S) \to REL(n,S)$.

LEMMA 3.2.37. $j_0, ..., j_1', ...$ are non surjective and E*1st/LMFR preserving on (S,FCN(1,S),...;REL(1,S),...).

Proof: This is from Lemma 3.2.36 via the isomorphism h:D → S which induces the isomorphism from (D,FCN(1,D),...;REL(1,D),...) onto (S,FCN(1,S),...;REL(1,S),...). QED

DEFINITION 3.2.27. W is a cumulation set if and only if
i. ∅ ∈ W.
ii. ∈|W is is a strict linear ordering.
iii. If y is the immediate successor of x in ∈|W then y = ℘(x).
iv. If x is a limit in ∈|W then x is the union of its predecessors in ∈|W.

LEMMA 3.2.38. W is a cumulation set if and only if it is $\{V(\gamma): \gamma < \beta\}$, for some $\beta > 0$.

Proof: Let W be a cumulation set. Then ∈|W is a well ordering of order type, say, β. Prove by transfinite induction on $\gamma < \beta$ that the γ-th element of W is V(γ). QED

LEMMA 3.2.39. There is a formula Δ in A*1st/LMFR, with exactly the free variable R ranging over REL(2,S), such that (∀R)(Δ ↔ R is isomorphic to some ∈|V(β)).

Proof: We say that fld(R) = ∅ or fld(R) ≠ ∅ and (fld(R),R) satisfies first the following conditions obviously expressible in 1st/LMFR:

1. Extensionality.
2. Foundation.
3. If there is no greatest ordinal or the greatest ordinal is a limit, then the sets are the subsets of the elements of cumulation sets.
4. If the greatest ordinal is a successor, then every element of every cumulation set has a power set, and the sets are the sets consisting of the subsets of the elements of cumulation sets.

Then we add second order separation:

5. Every *actual set* of R predecessors of a point forms the set of all R predecessors of a point.

Let Δ be fld(R) = ∅ ∨ (1 ∧ ... ∧ 5). Clearly every nonempty ∈|V(β) satisfies 1,2,5. We need to verify 3,4. If β is a limit then the cumulation sets which are elements of V(β) are the cumulation sets of length < β, and so the elements of V(β) are the subsets of their elements. If β = λ+1 then the cumulation sets in V(β) are the V(γ), γ ≤ λ, and so the elements of V(β) are the subsets of V(λ) and therefore the subsets of the elements of the cumulation sets in V(β). Finally, suppose β = γ+2. Then the cumulation sets in V(β) include the one ending with V(γ), because all of its elements lie in V(γ+1), and therefore it lies in V(γ+2). The cumulation set ending with V(γ+1) can't lie in V(γ+2) because it cannot be a subset of V(γ+1), whilst V(γ+1) ∈ V(γ+1), So the power set of any element of a cumulation set in V(β) lies in V(β). Also it is clear that the sets consisting of subsets of elements of V(γ) are exactly the elements of V(β).

Now let (fld(R),R) satisfy 1-5. Then (fld(R),R) is extensional and well founded. Let A be the unique transitive set such that (fld(R),R) ≈ (A,∈). By 6, every subset of every x ∈ A is an element of A. Let β be the set of ordinals in A. Then β is the least ordinal not in A. We show that A = V(β). It is clear that if A thinks W is a cumulation set then W is a cumulation set. This is because using 5, if W thinks x = ℘(y) then in fact x = ℘(y).

case 1. β is a limit. By 3, every γ < β is a subset of some cumulation set in A. Therefore there are cumulation sets in A of each length < β. There cannot be a cumulation set of length β because by 5, β would be an element of A. So A = V(β).

case 2. β = λ+1. By 3, λ is a subset of the union of a cumulation set C in A. C must be of length at least λ. Length λ+1 is impossible as by 5, λ+1 would be an element of A, which is impossible. So A consists of the subsets of V(λ), which means that A = V(λ+1). The internal subsets of V(λ) are the same as the subset of V(λ).

case 3. β = γ+2. γ+1 consists of subsets of an element of a cumulation set C ∈ E. So γ is a subset of an element of C. So V(γ) ∈ C. There cannot be a cumulation set in A with V(γ+1) as an element because the cumulation set is a subset of V(γ+1). By 4, A has an internal power set of V(γ) and this must be actual V(γ+1). By 4, A consists of the sets consisting of the subsets of V(γ), internally. Since V(γ+1) ∈ A, A consistas of the internal subsets of V(γ+1). Hence A = V(γ+2).

QED

DEFINITION 3.2.28. Fix Δ from Lemma 3.2.39. Fix T_0 = ∈|V(α).

LEMMA 3.2.40. j_0[fld(T_0)} ⊆ fld(j_2'(T_0)) = j_1'(fld(T_0)). T_0 = ∈|V(α) ≈ j_2'(T_0), where the isomorphism is unique.

Proof: For the first claim, we need x ∈ fld(T_0) → j_0(x) ∈ fld(j_2'(T_0)), which is immemdiate from 1st/LMFR preserving. Also fld(T_0) = fld(T_0). Treat T_0 as a parameter on the lefet side and fld(T_0) as a parameter on the right. Then by 1st/LMFR preserving, fld(j_2'(T_0)) = j_1'(fld(T_0)).

Thus $|\text{fld}(T_0)| \leq |\text{fld}(j_2'(T_0))|$. Now $\Delta(T_0)$, since $T_0 = \in|V(\alpha)$, by Lemma 3.2.39. Hence $\Delta(j2'(T_0))$ by A*1st/LMFR preserving. By Lemma 3.2.39, $j_2'(T_0)$ is isomorphic to some $\in|V(\beta)$. By the first claim, $|V(\alpha)| \leq |V(\beta)|$, and so $\alpha \leq \beta$ by the definition of α (Definition 3.2.26). Now $|\text{fld}(j_2'(T_0))| \leq |S| < |V(\alpha+1)|$ since $j_2'(T_0) \in \text{REL}(2,S)$. Hence $\alpha = \beta$ and so $\text{fld}(T_0)$ and $\text{fld}(j_2'(T_0))$ are of cardinality $|V(\alpha)|$. Therefore $T_0, j_2'(T_0)$ are both isomorphic to $\in|V(\alpha)$, and both isomorphisms are unique in this extensional well founded context. QED

DEFINITION 3.2.29. A binary relation R is a set of ordered pairs. fld(R) is the set of all coordinates of elements of R. We use a specific second order language for R's. We introduce the language BL2 for "binary logic second order". There is only a primitive binary relation symbol R, with = being understood. The first order variables v_i range over elements of fld(R). The second order variables A_i range over subsets of fld(R). The atomic formulas are $x_i = x_j$, $R(x_i,x_j)$, $x_i \in A_j$. The idea is that we can think of any binary relation R as a model for BL2 and do not need to form (dom(R),R). This simplification is worth making for our application, as it avoids needing to attend to certain details. Isomorphisms from R_1 onto R_2 are bijections h_0,h_1, $h_0:\text{fld}(R_1) \to \text{fld}(R_2)$, $h_1:\wp(\text{fld}(R_1)) \to \wp(\text{fld}(R_2))$, where $h_1(A) = h_0[A]$, such that $(\forall x,y \in \text{fld}(R_1))(R_1(x,y) \leftrightarrow R_2(h_0(x),h_0(y))$. R_1 and R_2 are isomorphic if and only if there exists an isomorphism from R_1 onto R_2. If R be a binary relation and E is a set then $R|E$ is $R \cap E^2$.

DEFINITION 3.2.30. The A*/BL2 statements applied to any binary relation R, take the form $(\forall A_1,\ldots,A_n \subseteq \text{fld}(R))(Qx_1\in\text{fld}(R))\ldots(Qx_m\in\text{fld}(R))(\varphi)$, with parameters $x_{m+1},\ldots,x_r \in \text{fld}(R)$ and parameters $A_{n+1},\ldots,A_s \subseteq \text{fld}(R)$. This matches the definition of Π_1 statements used in section 3.1 over the $V(\alpha+1)$. h_0,h_1 is A*/BL2 preserving from R_1 into R_2 if and only if $h_0:\text{fld}(R_1) \to \text{fld}(R_2)$ and $h_1:\wp(\text{fld}(R_1)) \to \wp(\text{fld}(R_2))$, where for all A*/BL2 statements φ with parameters $x_1,\ldots,x_n \in \text{fld}(R_1)$, $A_1,\ldots,A_m \subseteq \text{fld}(R_1)$, φ holds if and only if φ holds with parameters $h_0(x_1),\ldots,h_0(x_n) \in \text{fld}(R_1)$ and $h_1(A_1),\ldots,h_m(A_m) \subseteq \text{fld}(R_2)$.

LEMMA 3.2.41. j_0,j_1', suitably restricted, is A*/BL2 preserving from T_0 into $j_2'(T_0)$. The restrictions are to $fld(T_0)$ and $\wp(fld(T_0))$, which are $V(\alpha)$ and $V(\alpha+1)$.

Proof: We first verify that j_0 maps $fld(T_0) = V(\alpha)$ into $fld(j_2'(T_0))$. Let x be such that $T_0(x,y) \vee T_0(y,x)$. Then $j_2'(T_0)(j_0(x),j_0(y)) \vee j_2'(T_0)(j_0(y),j_0(x))$, and so $j_0(x) \in fld(j_2'(T_0))$. Next we verify that $A \subseteq fld(T_0) \rightarrow j_1'(A) \subseteq fld(j_2'(T_0))$. This is immediate from 1st/LMFR preserving treating A and T_0 as parameters.

Let φ be an A*/BL2 statement in T_0 with parameters $x_1,...,x_n \in fld(T_0)$, $A_1,...,A_m \subseteq fld(T_0)$. Assume that φ is expressed in the obvious way as an A*1st/LMF statement φ' by relativization, with parameters $x_1,...,x_k,A_1,...,A_m,T_0$. By A*1st/LMF preserving, φ' is equivalent to φ' with parameters $j_0(x_1),...,j_0(x_n),j_1'(A_1),...,j_1'(A_m),j_2'(T_0)$. By reversing the relativiation process, this is equivalent to $\varphi \in$ A*/BL2 in $j_2'(T_0)$ with parameters $j_0(x_1),...,j_0(x_n),j_1'(A_1),...,j_1'(A_m) \subseteq fld(j_2'(T_0))$. QED

DEFINITION 3.2.31. h_0,h_1 is the unique isomorphism from $j_2'(T_0)$ onto T_0. $j_0\hat{},j_1'\hat{}$ is the A*/BL2 preserving map from T_0 into $j_2'(T_0)$ given by Lemma 3.2.42.

LEMMA 3.2.42. h_0,h_1 is uniquely defined. $h_0j_0\hat{},h_1j_1'\hat{}$ is A*/BL2 preserving from T_0 into T_0.

Proof: h_0,h_1 is the uniquely defined as the inverse of the isomorphism given by Lemma 3.2.41. Thus $h_0:fld(j_0'(T_0)) \rightarrow fld(T_0)$, $h_1:\wp(fld(j_2'(T_0))) \rightarrow \wp(fld(T_0))$ are bijections and obviously h_0,h_1 is A*/BL2 preserving. And $j_0\hat{}:fld(T_0) \rightarrow fld(j_2'(T_0))$, $j_1\hat{}:\wp(fld(T_0) \rightarrow \wp(fld(j_2'(T_0))$ has $j_0\hat{},j_1\hat{}$ A*/BL2 preserving from T_0 into $j_2'(T_0)$. So we can compose. and so $h_0j_0\hat{},h_1j_1'\hat{}$ is A*/BL2 preserving from T_0 into T_0. QED

LEMMA 3.2.43. Let $A \subseteq S$. Suppose j_0 maps A onto $j_1'(A)$. Then j_1' maps $\wp(A)$ onto $\wp(j_1'(A))$ by forward imaging under j_0. In particular, every subset of $j_1'(A)$ is a value of j_1'.

Proof: Let j_0 map A onto $j_1'(A)$. Since j_0 is one-one, j_0 is a bijection from A onto $j_1'(A)$. Let $E \subseteq A$. Then $j_1'(E) \subseteq j_1'(A)$ by 1st/LMFR preserving. We claim that for all $x \in j_1'(A)$, $x \in j_1'(E) \leftrightarrow j_0^{-1}(x) \in E \leftrightarrow x \in j_0[E]$. The first equivalence is by 1st/LMFR preserving. The second equivalence is immediate. Hence $j_0[E] = j_1'(E)$. So j_1' maps $\wp(A)$ into $\wp(j_1'(A))$ by forward imaging by j_0, and since j_0 is a bijection from A onto $j_1'(A)$, j1' is a bijection from $\wp(A)$ onto $\wp(j_1'(A))$. QED

LEMMA 3.2.44. j_0^:fld(T_0) → fld($j_2'(T_0)$) is not surjective.

Proof: Suppose j_0^:fld(T_0) → fld($j_2'(T_0)$) is surjective. We claim that fld($j_2'(T_0)$) = j_1'(fld(T_0). To see this we view fld(T_0) = fld(T_0) as a statement with parameter T_0 on left and parameter fld(T_0) on right. Then fld($j_2'(T_0)$) = j_1'(fld(T_0)) by 1st/LMFR preserving. Hence j_0^:fld(T_0) → j_1'(fld(T_0)) is surjective, and we will apply Lemma 3.2.44. Since $2^{|fld(T0)|} = |V(\alpha+1)| \geq |S|$ (in fact, >) let W:S → $\wp$(fld(T_0)) be one-one. We convert W to the relation $W^* \subseteq S \times$ fld(T_0), where for all $x \in S$, $W^*_x = W(x)$. Thus the sections of W* are distinct subsets of fld(T_0). By 1st/LMFR preserving, the sections of $j_2'(W^*)$ are distinct subsets of j_1'(fld(T_0)). By Lemma 3.2.44 (last claim), the sections of $j_2'(W^*)$ are distinct values of j_1'. Let $x \in S$ be arbitrary. Then let $j_2'(W^*)_x = j_1'(A)$. Now $j_1'(A)$ is some section of $j_2'(W^*)$, and so by 1st/LMFR preserving, A is some W^*_u, and we fix u. By 1st/LMFR preserving, $j_1'(A) = j_2'(W^*)_{j(u)} = j_2'(W^*)_x$. So $x = j_0(u)$ because the sections of $j_2'(W^*)$ are distinct. But $x \in S$ was arbitrary. Therefore j_0:S → S is surjective. This is a contradiction. QED

LEMMA 3.2.45. h_0j_0,h_1j_1'^ is A*/BL2 preserving from T_0 into T_0. h_0j_0^:fld(T_0) → fld(T_0) is not surjective.

Proof: First claim copied from Lemma 3.2.42. h_0:fld($j_2'(T_0)$) → fld(T_0), h_2:$\wp$(fld($j_2'(T_0)$) → $\wp$(fld(T_0)) is a bijection by Definition 3.2.31 and Lemma 3.2.42, and by Lemma 3.2.44, j_0^:fld(T_0) → fld($j_2'(T_0)$) is not surjective. Clearly h_0j_0^:fld(T_0) → fld(T_0) is not surjective. QED

LEMMA 3.2.46. There exists a nontrivial f:V(α+1) → V(α+1) which is elementary for Π_1 formulas.

Proof: By Lemma 3.2.45, we have g:V(α) → V(α), h:V(α+1) → V(α+1), g not surjective, where g,h is A*/BL2 preserving from $\in|V(\alpha)$ into $\in|V(\alpha)$. Let $x \in V(\alpha)$. Also $x = A \subseteq V(\alpha)$. Now $(\forall y \in V(\alpha))(y \in x \leftrightarrow y \in A)$. Hence $(\forall y \in V(\alpha)(y \in g(x)$

↔ y ∈ h(A)) since g,h are A*/BL2 preserving. Hence g(x) = h(A) = h(x). Therefore g ⊆ h. Since g is not surjective, g is nontrivial and hence h is nontrivial. So from the matching definition of Π_1 formulas (statements) in section 3.1, we see that h:V(α+1) → V(α+1) is nontrivial and elementary for Π_1 formulas. QED

THEOREM 3.2.47. (NBG + AxC) Some symmetric semigroup has a non surjective solvable equation preserving mapping if and only if I2 holds. (ZFC) Some symmetric semigroup has a non surjective solvable equation preserving mapping if and only if I2'' holds if and only if I2' holds.

Proof: By Theorem 3.1.2 and Lemma 3.2.46. QED

We now give some more precise information.

THEOREM 3.2.48. If λ is an I2 cardinal then there is a non surjective solvable equation preserving mapping of λλ. If there is a non surjective solvable equation preserving mapping of DD then there is an I2 cardinal $\lambda \leq |D| < 2^\lambda$.

Proof: The first claim is by Theorem 3.1.4. Suppose there is a non surjective solvable equation preserving mapping on DD. Recall α is greatest such that |V(α)| ≤ |D|, and by Lemma 3.2.46, α is an I2 ordinal. By Theorem 3.1.3, claim 2, α is an ω limit of strongly inaccessible cardinals. Hence $\alpha = |V(\alpha)| \leq |D| < |V(\alpha+1)| = 2^{|V(\alpha)|} = 2^\alpha$. QED

4. ELEMENTARY EMBEDDING (symmetric semigroups)

4.1. DERIVATION FROM I1

The strongest of the commonly quoted large cardinal hypotheses is I1.

I1. There is a nontrivial elementary embedding j:V(λ+1) → V(λ+1).

THEOREM 4.1.1. ZFC + I1 proves the existence of a symmetric semigroup with a non surjective elementary embedding. If there is a nontrivial elementary embedding from V(λ+1) into

V(λ+1) then the symmetric semigroup (λλ,•) has a non surjective elementary embedding.

Proof: Let j:V(λ+1) → V(λ+1) be a nontrivial elementary embedding with critical point κ. Every f:λ → λ is a set of ordered pairs drawn from V(λ), and such order pairs are elements of V(λ). Also for all f:λ → λ, j(f):λ → λ. Hence j:λλ → λλ.

Now let id(κ) be the element of λλ that is constantly κ. We claim that id(κ) cannot be a value of j. For if j(f) = i(κ) then j(f) is constant, and so f is constant. Now j(f)(0) = i(κ)(0) = κ = j(f)(j(0)) = j(f(0)). Since κ ∉ rng(j), we have a contradiction.

It remains to show that j is an elementary embedding of the symmetric semigroup λλ. Let $\varphi(x_1,...,x_n)$ be a first order statement over the semigroup λλ with parameters $x_1,...,x_n \in$ λλ ⊆ V(λ+1). Then $\varphi(x_1,...,x_n)$ is a first order statement over V(λ+1) with parameters from V(λ+1). Therefore $\varphi(x_1,...,x_n) \leftrightarrow \varphi(j(x_1),...,j(x_n))$ by the elementarity of j. QED

It is immediate from this construction that the identity is preserved - although by Lemma 3.2.8 we know that it is automatic for symmetric semigroups even if we only assume solvable equation preserving.

THEOREM 4.1.2. If λ is an I1 cardinal then there is a non surjective elementary embedding of λλ.

Proof: By the proof of Theorem 4.1.1. QED

4.2. DERIVATION OF I1

We now start with a non surjective logic preserving mapping j on a symmetric semigroup DD. We derive I1. This is the same as j being a non surjective elementary embedding with respect to the language LSG.

DEFINITION 4.2.1. We fix a symmetric semigroup (DD,•) and a non surjective elementary embedding j_1:(DD,•) → (DD,•). It will become clear below why we write j_1 instead of j.

DEFINITION 4.2.2. We use LUF and accessories as given in Definitions 3.2.4 - 3.2.7. For x ∈ D, x* is constantly x. C = {x*: x ∈ D}. For f ∈ C, v(f) is the constant value of f. For f ∉ C, v(f) is undefined. j_0:D → D is given by j_0(x) = v(j_1(x*)).

LEMMA 4.2.1. j_0,j_1 is an elementary embedding from (D,DD,•,A) into (D,DD,•,A). j_0 is not surjective.

Proof: The first claim is by a much more straightforward exploitation of interpreting elements of D by constant functions (x to x*) than was exploited by Lemma 3.2.10. For the second claim see Lemma 3.2.9 claim 9. QED

DEFINITION 4.2.3. Fix P[i,n], 1 ≤ i ≤ n, n ≥ 2, such that for all (∀x_1,...,x_n ∈ D)(∃!y)(∀i ≤ n)(P]i,n](y) = x_i). Write <x_1,...,x_n>P for this unique y.

DEFINITION 4.2.4. We use LMF and accessories as given in Definitions 3.2.18 - 3.2.21.

LEMMA 4.2.2. Let F:D^n → D, n ≥ 2. UN(F,P) ∈ DD is given by UN(F,P)(x) = F(P[1,n](x),...,P[n,n](x)).

LEMMA 4.2.3. Let n ≥ 2. F(x_1,...,x_n) = UN(F,P)(<x_1,...,x_n>P). The operation that sends F ∈ FCN(n,D) to UN(F,P) is a bijection from FCN(n,D) onto DD. This holds no matter what alternative P[i,n] that we use, as long as it obeys the condition given in Definition 4.2.3.

Proof: See Lemma 3.2.28. QED

LEMMA 4.2.4. For every formula φ in LMF with free variables at most x_1,...,x_n,f_1,...,f_m,G_1,...,G_r, G's of various arity ≥ 2, there is a formula ψ in LUF with free variables at most x_1,...,x_n,f_1,...,f_m,g_1,...,g_r such that (∀x_1,...,x_n)(∀f_1,...,f_m)(∀g_1,...,g_r)(∀G_1,...,G_r)(UN(G_1,P) = g_1 ∧ ... ∧ UN(G_r,P) = g_r → (φ ↔ ψ)) holds universally.

Proof: See Lemma 3.2.33. QED

DEFINITION 4.2.5. For n ≥ 2, we define j_n:FCN(n,D) → FCN(n,D) as follows. j_n(F) ∈ FCN(n,D) is unique such that UN(j_n(F),P') = j_1(UN(F,P)).

LEMMA 4.2.5. j_n:FCN(n,D) → FCN(n,D) is uniquely defined by Definition 4.2.5.

Proof: See Lemma 3.2.34. QED

LEMMA 4.2.6. j_0,j_1,j_2,... is an elementary embedding from (D,FCN(1,D),FDN(2,D),...) into (D,FCN(1,D),FCN(2,D),...) for LMF.

Proof: See Lemma 3.2.35. The only part of the active parameter, parameter equivalent, alternative parameter facility of section 3.2 that we need is the P[i,n]. Since we have elementary embedding, the j_n(P)[1,n] being alternative is trivial here. QED

DEFINITION 4.2.6. We expand the language LMF to LMFR = language of multivariate functions and relations with sorts S,FCN(1,S),FCN(2,S),...,REL(1,S),REL(2,S),..., as in Definition 3.2.25.

DEFINITION 4.2.7. For F ∈ FCN(n,S), define rel(F) = {(x_1,...,x_n):F(x_1,...,x_n) = x_1}. We define j_n':REL(n,S) → REL(n,S) by j_n'(A) = rel(j_n(F)) where rel(F) = A.

LEMMA 4.2.7. Each j_n' is well defined. j'(rel(F)) = rel(j(F)). j_0,...,j_1',... is an LMFR elementary embedding from (S,FCN(1,S),FCN(2,S),...,REL(1,S),REL(2,S),...) into (S,FCN(1,S),FCN(2,S),...,REL(1,S),REL(2,S),...).

Proof: See Lemma 3.2.36. QED

DEFINITION 4.2.8. We move our j's to a convenient set S of the same cardinality as D via an arbitrary bijection h:D → S. We choose our S as follows. Let α be the greatest ordinal such that $|V(\alpha)| \leq |D|$. Let $V(\alpha) \subseteq S \subseteq V(\alpha+1)$, where |S| = |D|. So we have j_0*,...,j_1'*,... as in Lemma 3.2.36, this time on S,FCN(1,S),...,REL(1,S),... . We leave the *'s off and write j_0,...,j_1',.., where j_0:S → S, j_n:FCN(n,S) → FCN(n,S), j_n':REL(n,S) → REL(n,S).

LEMMA 4.2.8. j_0,...,j_1',... are non surjective and E*1st/LMF preserving on (S,FCN(1,S),...;REL(1,S),...).

Proof: Via the isomorphism h:D → S as in Lemma 3.2.37. QED

LEMMA 4.2.9. j_0[fld(T_0)} ⊆ fld(j_2'(T_0)) = j_1'(fld(T_0)). T_0 = ∈|V(α) ≈ j_2'(T_0), where the isomorphism is unique.

Proof: See Lemma 3.2.40. Can be greatly simplified because of the elementary embedding. QED

DEFINITION 4.2.9. The BL2 statements applied to any binary relation R, take the form
$(QA_1 \subseteq fld(R))\ldots(QA_k \subseteq fld(R))(Qx_1 \in fld(R))\ldots(Qx_m \in fld(R)(\varphi)$,
with parameters $x_{m+1},\ldots,x_r \in$ fld(R) and parameters $A_{n+1},\ldots,A_s \subseteq$ fld(R), where the atomic formulas are $x_i = x_j$, $x_i \in x_j$, $x_i \in A_j$.

LEMMA 4.2.13. j_0,j_1', suitably restricted, is A*/BL2 preserving from T_0 into j_2'(T_0). The restrictions are to fld(T_0) and ℘(fld(T_0), which are V(α) and V(α+1).

Proof: See Lemma 3.2.41. QED

DEFINITION 4.2.11. h_0,h_1 is the unique isomorphism from j_2'(T_0) onto T_0. j_0,j_1'^ is the A*/BL2 preserving map from T_0 into j_2'(T_0) given by Lemma 3.2.42.

LEMMA 4.2.14. h_0,h_1 is uniquely defined. h_0j_0,h_1j_1'^ is A*/BL2 preserving from T_0 into T_0.

Proof: See Lemma 3.2.42. QED

LEMMA 4.2.15. Let A ⊆ S. Suppose j_0 maps A onto j_1'(A). Then j_1' maps ℘(A) onto ℘(j_1'(A)) by forward imaging under j_0. In particular, every subset of j1'(A) is a value of j_1'.

Proof: See Lemma 3.2.43. QED

LEMMA 4.2.16. j_0^:fld(T_0) → fld(j_2'(T_0)) is not surjective.

Proof: See Lemma 3.2.44. QED

LEMMA 4.2.17. h_0j_0,h_1j_1'^ is BL2 preserving from T_0 into T_0. h_0j_0^:fld(T_0) → fld(T_0) is not surjective.

Proof: See Lemma 3.2.45. QED

LEMMA 4.2.18. There exists a nontrivial elementary f:V(α+1) → V(α+1).

Proof: See Lemma 3.2.46. QED

THEOREM 4.2.19. Some symmetric semigroup has a non surjective elementary embedding if and only if I1 holds.

Proof: By Theorem 4.1.1 and Lemma 4.2.18. QED

We now give some more precise information.

THEOREM 4.2.20. If λ is an I1 cardinal then there is a non surjective elementary embedding of $\lambda\lambda$. If there is a non surjective elementary embedding of DD then there is an I1 cardinal $\lambda \leq |D| < 2^{\lambda}$.

Proof: The first claim is by Theorem 4.1.2. Suppose there is a non surjective elementary embedding of DD. Recall α is greatest such that $|V(\alpha)| \leq |D|$, and by Lemma 4.2.18, α is an I1 ordinal. By Theorem 3.1.3, claim 1, α is an ω limit of strongly inaccessible cardinals. Hence $\alpha = |V(\alpha)| \leq |D| < |V(\alpha+1)| = 2^{|V(\alpha)|} = 2^{\alpha}$. QED

5. ABSOLUTELY PRESERVING

Finally we come to absolute preserving, Definition 1.1.6. We shall see that all absolutely preserving mappings on all symmetric semigroups are surjective. The proof is clear enough that we will make this section self contained and not rely on sections 3.2 or 4.2. We could rely on them because obviously any absolutely preserving mapping is E*= preserving and even an elementary embedding.

We fix a set D with an absolutely preserving $j:DD \to DD$. We show that j is surjective.

DEFINITION 5.1. For $d \in D$, let $d^* \in DD$ be constantly d. Let $C = \{d^*: d \in D\}$.

LEMMA 5.1. $f \in C \leftrightarrow (\forall g)(f = fg)$. j is one-one. $j:C \to C$.

Proof: For the first claim, if $f \in C$ then $f = fg$ is obvious. Suppose $(\forall g)(f = fg)$. Suppose $f(a) \neq f(b)$. Let $g(a) = b$. Then $f(a) = fg(a) = f(b)$, a contradiction. The next two claims follow immediately from (j being an) elementary embedding. QED

DEFINITION 5.2. P_1,P_2 is a pairing pair if and only if $(\forall x,y \in D)(\exists! z)(P_1(z) = x \wedge P_2(z) = y)$. $<x,y>P$ is the unique z such that $P_1(z) = x \wedge P_2(z) = y$.

LEMMA 5.2. If D is infinite then there is a pairing pair.

Proof: Let $h:D \rightarrow D^2$ be a bijection. For each $d \in D$ set $P_1(d),P_2(d)$ to be such that $h(d) = (P_1(d),P_2(d))$. QED

We can henceforth assume that D is infinite because if D is finite then obviously j is surjective (by Lemma 5.1).

DEFINITION 5.3. We fix a pairing pair P_1,P_2. We fix a well ordering $(D,<)$ of order type $|D|$. Define $WO[1]:D \rightarrow D$ by $WO[1](d) = P_1(d)$ if $P_1(d) < P_2(d)$; $P_2(d)$ otherwise.

LEMMA 5.3. $<x,y>P$ is onto D. The binary relation "$WO[1](<x,y>P) = x \wedge x \neq y$" in variables x,y and parameters $WO[1],P_1,P_2$, is <.

Proof: For the first claim let $z \in D$. Then $<P_1(z),P_2(z)>P = z$. For the second claim, let $x,y \in D$. Then $WO[1](<x,y>P) = P_1(<x,y>P)$ if $P_1(<x,y>P) < P_2(<x,y>P)$; $P_2(<x,y>P)$ otherwise. I.e., $WO[1](<x,y>P) = x$ if $x < y$; y otherwise. So if $x < y$ then $WO[1](<x,y>P) = x \wedge x \neq y$. If $x = y$ then $\neg(WO[1](<x,y>P) = x \wedge x \neq y)$. If $x > y$ then $WO[1](<x,y)P) = P_2(<x,y>P) = y$, and so also $\neg(WO[1](<x,y>P) = x \wedge x \neq y)$. This establishes the second claim. QED

LEMMA 5.4. The relation "P_1,P_2 is a pairing pair $\wedge$ the relation "$WO[1](<x,y>P) = x \wedge x \neq y$" is a well ordering on D of type $|D|$, in variables $WO[1],P_1,P_2$ with no parameters, is first order over $(DD,\bullet)$.

Proof: P_1,P_2 is a pairing pair if and only if $(\forall x,y \in D)(\exists! z)(P_1(z) = x \wedge P_2(z) = y)$. We claim this is equivalent to $(\forall f,g \in C)(\exists! h \in C)(P_1h = f \wedge P_2h = g)$. To see this, assume $(\forall x,y \in D)(\exists! z)(P_1(z) = x \wedge P_2(z) = y)$ and let $f,g \in C$. Write $f = x^* \wedge g = y^*$. Let $P_1(z) = x \wedge P_2(z) = y$. Set $h = z^*$. Now suppose $P_1w^* = x^* \wedge P_2w^* = y^*$. Then $P_1(w) = x \wedge P_2(x) = y \wedge w = z$. Finally conversely suppose $(\forall f,g \in C)(\exists! h \in C)(P_1h = f \wedge P_2h = g)$ and let $x,y \in D$. Then $(\exists! h \in C)(P_1h = x^* \wedge P_2h = y^*)$. Let $h = z^*$. Then $P_1(z) = x \wedge P_2(z) = y$. Suppose $P_1(w) = x \wedge P_2(w) = y$. Then $P_1w^* = x^* \wedge P_2w^* = y^*$ and so $w^* = z^*$, $w = z$. This establishes the claim. And by Lemma 5.1, membership in C is first order over (DD,•) without parameters. So being a pairing pair is first order over (DD,•) without parameters. Hence "$WO[1](<x,y>P) = x \wedge x \neq y$" is a linear ordering on D, is first order over (DD,•) without parameters in variables $WO[1],P_1,P_2$.

We now want to say "$WO[1](<x,y>P) = x \wedge x \neq y$" is a well ordering on D in variables $WO[1],P_1,P_2$, with no parameters. We can say that every nonempty range of an element of DD has a least element for this linear ordering on D. But we have to interpret this appropriately with constant functions. Note that $x^* \in rng(f)$ if and only if $(\exists y^*)(fy^* = x^*)$. So then we need only give a first order definition of x^*,y^* are such that "$WO[1](<x,y>P) = x \wedge x \neq y$". We can write $(\exists z^*)(WO[1]z^* = x^* \wedge x^* \neq y^* \wedge z^* = (<x,y>P)^*)$, where $z^* = (<x,y>P)^*$ if and only if $P_1z^* = x^* \wedge P_2z^* = y^*$.

Finally we need to say that "$WO[1](<x,y>P) = x \wedge x \neq y$" has order type $|D|$. This is the same as saying that there is no one-one map γ from D with a strict upper bound. Similar considerations as above allows us to do this appropriately in terms of constant functions and a general function $\gamma \in DD$. QED

LEMMA 5.5. The statement "P_1,P_2 is a pairing pair $\wedge$ the relation "$WO[1](<x,y>P) = x \wedge x \neq y$" is a well ordering on D of type $|D|$" with parameters $WO[1],P_1,P_2$, is true. Furthermore it is also true with parameters $j(WO[1]),j(P_1),j(P_2)$.

Proof: The first claim is by Lemma 5.3. The second claim is by elementary embedding. QED

DEFINITION 5.4. Let R_1 be the linear ordering on D, "$WO[1](<x,y>P) = x \wedge x \neq y$", using parameters $WO[1],P_1,P_2$, and R_2 be the linear ordering on D, "$j(WO[1])(<x,y>j(P) = x \wedge x \neq y$" using parameters $j(WO[1]),j(P_1),j(P_2)$. Let R_1^*,R_2^* be the corresponding relations on C. I.e., $R_1^*,R_2^* \subseteq C_2$, $R_1^*(x^*,y^*) \leftrightarrow R_1(x,y)$, and $R_2^*(x^*,y^*) \leftrightarrow R_2(x,y)$.

LEMMA 5.6. R_1,R_2 are well orderings of D of order type |D|. R_1*,R_2* are well orderings of C of order type |D|. R_1*,R_2* can be given the same first orer definition over (D,•) but with the parameters WO[1],P_1,P_2 changed to j(WO[1]),j(P_1),j(P_2). There is a unique isomorphism h from (D,R_1) onto (D,R_2), and a unique isomorphism h* from (C,R_1*) onto (C,R_2*). Here h*(x*) = h(x)*.

Proof: By Lemma 5.5. Obviously any two well orderings of D of order type |D| are uniquely isomorphic. QED

DEFINITION 5.5. Let h,h* be the unique isomorphisms of (D,R1) onto (D,R2) and (C,R_1*) onto (C,R_2*), respectively, given by Lemma 5.8.

So far, we have not used absolutely preserving. We better use it to get our contradiction because otherwise, in light of Theorem 4.1.2, we would be refuting I1. In fact we have deliberately taken argument as far as we naturally can just using elementary embedding.

LEMMA 5.7. Every j(x*) = h*(x*). I.e., j = h* on C.

Proof: Let x ∈ D. j sends WO[1],P_1,P_2,x* to j(WO[1]),j(P_1),j(P_2),j(x*). Hence by absolute preserving, there is an isomorphism α from (DD,•,WO[1],P_1,P2,x*) onto (DD,•,j(WO[1]),j(P_1),j(P_2),j(x*)). Now since R_1* is definable in (DD,•,WO[1],P_1,P_2) without parameters and R_2* is definable in the same way in (DD,•,j(WO[1]),j(P_1),j(P_2)) without parameters, α|C must be an isomorphism from R_1* onto R_2*. But the unique such α|C is h*. Now obviously α(x*) = j(x*), and so h*(x*) = j(x*). Since x is arbitrary, j = h* on C. QED

LEMMA 5.8. j maps C onto C. j is surjective.

Proof: For the first claim, since h* is a bijection of C, and j = h* on C, we see that j maps C onto C. By Lemma 3.2.9, claim 10, if j is not surjective then j does not map C onto C. (Section 3.2 is based solely under the assumption that j is an elementary embedding of DD and is not surjective). Hence j is surjective. QED

THEOREM 5.9. Every absolutely preserving mapping on a symmetric semigroup is surjective.

Proof: By Lemma 5.8. QED

6. GENERAL PERSPECTIVES

In [Fr04] we found a number of very basic statements about extensions of general structures that preserve small substructures up to isomorphism, and related statements involving proper elementary extensions with respect to weak second order logic, that are equivalent to a measurable cardinal. Here we open up a new line with statements about embeddings of, specifically, the symmetric semigroups, that preserve statements, where we have equivalence with the far stronger large cardinal hypotheses I2 and I1.

The reason such elementary statements can be equivalent to large cardinal hypotheses is that the structures considered are on arbitrary sets. We believe that something like this can be done even for countable structures, finitely generated structures, and even finite structures, of a transparent algebraic nature, where the equivalence is with the consistency of large cardinal hypotheses. We don't expect the formulations to be as simple as the ones here and in [Fr04], but we still expect them to be remarkably simple and thematic in nature, graphically illustrating the great power and necessary use of large cardinal hypotheses.

REFERENCES

[Fr04] Working with Nonstandard Models, Nonstandard Models of Arithmetic and Set Theory, Ali Enayat and Roman Kossak, Editors, Contemporary Mathematics, vol. 361. https://cpb-usw2.wpmucdn.com/u.osu.edu/dist/1/1952/files/2014/01/Balt073103-21hprsq.pdf

[Ka94] Kanamori, Akihiro (2003), The Higher Infinite : Large Cardinals in Set Theory from Their Beginnings (2nd ed.), Berlin, New York: Springer-Verlag, doi:10.1007/978-3-540-88867-3, ISBN 978-3-540-00384-7.

[Ku71] Kenneth Kunen, (1971), "Elementary embeddings and infinitary combinatorics", *Journal of Symbolic Logic*, 36 (3): 407–413, doi:10.2307/2269948, JSTOR 2269948, MR