SOME HIGHLY UNDECIDABLE LATTICES

Menachem MAGIDOR
Hebrew University, Jerusalem, Israel

John W. ROSENTHAL
Ithaca College, Ithaca, NY 14850, USA

Mattiya hu RUBIN
Ben Gurion University, Beersheva, Israel

Gabriel SROUR
Simon Fraser University, Burnaby, B.C., Canada

Communicated by A. Nerode
Received 9 September 1988

Introduction

Let S be a Steinitz Exchange System with closure operation cl (see e.g. [5] for definitions). In this paper we examine the logical complexity of the first-order theory of the lattice of cl-closed subsets of S. (In the first-order language for lattices we use symbols for meet, join, and the elements zero and one.) As quantification over the elements of the lattice is quantification over some of the subsets of S, it is conceivable that this theory has the complexity of full second-order logic on the set S. (By second-order logic we mean allowing quantification over elements of S and also for each n over all n-ary relations on S.) We show that in many cases the first-order theory of the lattice has the complexity of full second-order logic on S.

The strongest results are in the special case where S is an algebraically closed field and cl is algebraic closure in S. We show:

Theorems 1.6 and 3.1. Let K be an algebraically closed field of infinite transcendence degree over its prime field. Then the first-order theory of the lattice of algebraically closed subfields of K has the strength of full second-order logic on the set K.

That is, loosely speaking, this lattice is as undecidable as possible.

In Section 1 we prove this result in characteristic 0 both because the proof is simpler and because the proof illustrates some of the results in Section 2. In Section 3 we modify this proof to work in any characteristic.

For general Steinitz Exchange Systems we want to avoid trivial second-order theories that arise when \( \text{cl}(X) = X \) for all \( X \). We do this by making the additional assumption that the Steinitz exchange system is nontrivial, that is, if \( x \) and \( y \) are independent over \( A \), then

\[
\text{cl}_A(\{x, y\}) \supseteq \text{cl}_A(\{x\}) \cup \text{cl}_A(\{y\}), \quad \text{where} \quad \text{cl}_A(B) = \text{cl}(A \cup B).
\]

In Section 2 we prove:

**Theorem 2.13.** Let \( S \) be a nontrivial, Steinitz exchange system of infinite dimension over \( \emptyset \). Then the first-order theory of the lattice of closed substructures of \( S \) is of complexity at least that of second-order logic on \( \aleph_0 \) (or equivalently, second-order number theory).

**Section 1**

Let \( K \) be an algebraically closed field of characteristic 0 and infinite transcendence degree over \( \mathbb{Q} \), the rationals. Let \( k = \text{cl}(\mathbb{Q}) \). Let \( \mathcal{L} \) be the lattice of algebraically closed subfields of \( K \). Let \( \mathcal{L}^* \) consist of \( \mathcal{L} \) together with several parameters, that is, constant symbols for several elements of \( \mathcal{L} \) to be introduced shortly. We first show that \( \mathcal{L}^* \) has the logical complexity of second-order logic on \( K \), and then we show how to eliminate the use of these parameters.

Let \( B = \{b_i : i \in I\} \) be a transcendence basis of \( K \) over \( k \). As \( K \) is of infinite transcendence degree, \( K \) and \( I \) have the same cardinality. Thus, it suffices to show how to translate all sentences of second-order logic on \( I \) into sentences of the first-order theory of \( \mathcal{L}^* \) (and later on \( \mathcal{L} \)). Furthermore, by folklore it suffices to show how to translate into sentences of the first-order theory of \( \mathcal{L}^* \) only those sentences of second-order logic with quantification over elements of \( I \) and quantification over functions from \( I \) to \( I \).

**Notation.** For any subset \( \{w_j : j \in J\} \) of \( K \), we let \((w_j : j \in J)\) denote \( \text{cl}(\{w_j : j \in J\}) \). Similarly for any element \( w \) of \( K \), we let \((w)\) denote \( \text{cl}(\{w\}) \).

Say \( x_1, \ldots, x_n \) are algebraically independent elements of \( K \). Say \( x \in (x_1, \ldots, x_n) \). We say \( x \) depends on \( x_1, \ldots, x_n \) if \( x_i \in (x_1, \ldots, x_n) \) with \( x_i \) replaced by \( x \) for \( i = 1, \ldots, n \).

\( B \) can be split into two disjoint subsets \( B_X = \{x_i : i \in I\} \) and \( B_Y = \{y_i : i \in I\} \). The parameters are \( K^*_X = (B_X) \), \( K^*_Y = (B_Y) \), \( K^*_F = (x_i + y_i : i \in I) \), and \( K^*_F = (x_i, y_i : i \in I) \).

Let \( \text{Id}(u, v) \) be the formula in the language of lattices that says:

- \( (i) \) \( u \) is one dimensional contained in \( K^*_X \)
- \( (ii) \) \( v \) is one dimensional contained in \( K^*_Y \)
- \( (iii) \) \( (u \text{ join } v) \text{ meet } K^*_F \) is one dimensional
- \( (iii) \) \( (u \text{ join } v) \text{ meet } K^*_F \) is one dimensional.
(It should be noted that the statement “w is one dimensional” is expressible in the first-order language of lattices.)

**Proposition 1.1.** \( \text{Id}(u, v) \) if and only if there is an \( i \in I \) such that \( u = (x_i) \) and \( v = (y_i) \).

**Proof.** A crucial tool in the study of the lattice \( L \) is a characterization of transcendence degree using formal derivatives. This was also used in [2] in prior work on this lattice, and in [1] in work on undecidability, where it was shown that the theory of algebraically closed fields with added relation symbols for algebraic independence is undecidable. The characterization is:

If \( x_1, \ldots, x_n \) are algebraically independent and \( u_1, \ldots, u_m \in (x_1, \ldots, x_n) \), then the transcendence degree of \( (u_1, \ldots, u_m) \) is the rank of the Jacobian matrix:

\[
\left( \frac{\partial u_j}{\partial x_i} \right)_{i=1, \ldots, n \text{ and } j=1, \ldots, m}
\]

where, \( \partial u_j/\partial x_i \) is a formal derivative, which we will also denote as \( (u_j)_x \). We denote this Jacobian as \( J(u_1, \ldots, u_m; x_1, \ldots, x_m) \). A detailed description is given in [3].

**Lemma 1.2.** \( \text{Id}(x_i, y_i) \).

**Proof.** (ia) and (ib) hold trivially for \( u = (x_i) \) and \( v = (y_i) \).

As \( x_i + y_i \in (x_i) \) join \( (y_i) \), \( (x_i) \) join \( (y_i) \) meet \( K^* \) has dimension at least 1. We assume the dimension is greater than 1. Hence \( x_i \) and \( y_i \) are elements of \( K^* \). This is impossible as \( x_i \) and the \( x_j + y_j \)'s are algebraically independent. For example, one can show that \( x_1, x_1 + y_1, \ldots, x_n + y_n \) are algebraically independent by examining the Jacobian \( J(x_1, x_1 + y_1, \ldots, x_n + y_n; x_1, \ldots, x_n, y_1, \ldots, y_n) \). It is

\[
\begin{bmatrix}
1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 & 0 & 1 & \cdots & 0 \\
0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 1
\end{bmatrix}
\]

This has rank \( n + 1 \).

We have shown that (ii) holds for \( u = (x_i) \) and \( v = (y_i) \). Similarly (iii) holds for \( u = (x_i) \) and \( v = (y_i) \). \( \square \)

**Lemma 1.3.** (ia), (ib), and (ii) imply that there exist \( x^* \) and \( y^* \) identical k-linear combinations of the \( x_i \)'s and the \( y_i \)'s respectively such that \( u = (x^*) \) and \( v = (y^*) \).

**Proof.** Say \( u = (x) \) and \( v = (y) \). By renaming indices we can assume \( x \in (x_1, \ldots, x_n) \) and \( y \in (y_1, \ldots, y_n) \).
Claim. $x, x_1 + y_1, \ldots, x_n + y_n$ are algebraically independent.

For if not, then the Jacobian

$$J(x, x_1 + y_1, \ldots, x_n + y_n; x_1, \ldots, x_n, y_1, \ldots, y_n)$$

has rank $n$. By an elementary linear algebra argument, $(x)_i = 0$ for $i = 1, \ldots, n$. And hence, $x$ is algebraic. This contradicts that $(x)$ has dimension 1.

Similarly $y, x_1 + y_1, \ldots, x_n + y_n$ are algebraically independent.

Claim. $x, y, x_1 + y_1, \ldots, x_n + y_n$ are algebraically dependent.

For if they are algebraically independent, then $(x, y)$ join $K^*$ has dimension 0. This contradicts (ii).

Thus, we may conclude that the following Jacobian has rank $n + 1$:

$$J(x, y, x_1 + y_1, \ldots, x_n + y_n; x_1, \ldots, x_n, y_1, \ldots, y_n)$$

We denote the first row as $\nabla_x x$, and the second row as $\nabla_y y$. We denote the remaining rows as $e_1, \ldots, e_n$.

As $y, x_1 + y_1, \ldots, x_n + y_n$ are algebraically independent, the last $n + 1$ rows are algebraically independent. Hence $\nabla_x x$ is a $K$-linear combination of $\nabla_y y, e_1, \ldots, e_n$. That is, $\nabla_x x = c \nabla_y y + c_1 e_1 + \cdots + c_n e_n$, where $c, c_1, \ldots, c_n$ are elements of $K$. The $i$th column of the Jacobian implies $c_i = (x)_i$. The $(n + i)$th column of the Jacobian implies $0 = c(y)_{y_i} + (x)_{x_i}$.

Claim. $c \neq 0$.

For assume $c = 0$. Then $(x)_i = 0$ for $i = 1, \ldots, n$. So $x$ is algebraic. This contradicts (i).

As $c \neq 0$, $(x)_i = 0$ if and only if $(y)_{y_i} = 0$. This implies that $x$ and $y$ depend on precisely the same $x_i$'s and $y_i$'s respectively. So we may as well assume that $x$ depends on $x_1, \ldots, x_n$. 

44 M. Magidor et al.
Thus, for \( i = 1, \ldots, n \) we have
\[
\begin{align*}
(x)_{x_i} & = (y)_{y_i} \\
(x)_{y_i} & = (y)_{y_i},
\end{align*}
\]
Let \( r_i \) be this common ratio. So \( r_i \in K_x^* \cap K_y^* \), which is \( k \), since \( x_1, \ldots, x_n, y_1, \ldots, y_n \) are algebraically independent.

**Claim.** \( u = (x*) \) where \( x^* = r_1x_1 + \cdots + r_nx_n \).

We just observe that \( x \) and \( x^* \) are algebraically dependent since
\[
J(x, x^*; x_1, \ldots, x_n, y_1, \ldots, y_n) = \begin{bmatrix}
(x)_{x_1} & \cdots & (x)_{x_n} \\
r_1 & \cdots & r_n
\end{bmatrix}
\]
has rank 1.

Similarly \( v = (y*) \) where \( y^* = r_1y_1 + \cdots + r_ny_n \).

**Proof of Proposition 1.1** (continued). Let \( x \) and \( y \) be as in the proof of Lemma 1.3. We may assume \( x = x^* \) and \( y = y^* \).

Reasoning as in the proof of Lemma 1.3 one can show that
\[
x, x_1y_1, \ldots, x_ny_n \text{ are algebraically independent and that} \\
y, x_1y_1, \ldots, x_ny_n \text{ are algebraically independent, but that} \\
x, y, x_1y_1, \ldots, x_ny_n \text{ are algebraically dependent.}
\]
Thus,
\[
J(x, y, x_1y_1, \ldots, x_ny_n; x_1, \ldots, x_n, y_1, \ldots, y_n) = \begin{bmatrix}
(x)_{x_1} & (x)_{x_2} & \cdots & (x)_{x_n} & 0 & 0 & \cdots & 0 \\
0 & 0 & \cdots & 0 & (y)_{y_1} & (y)_{y_2} & \cdots & (y)_{y_n} \\
y_1 & 0 & \cdots & 0 & x_1 & 0 & \cdots & 0 \\
0 & y_2 & \cdots & 0 & 0 & x_2 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & y_n & 0 & 0 & \cdots & x_n
\end{bmatrix}
\]
has rank \( n + 1 \). The first two rows are again \( \nabla_x x \) and \( \nabla_y y \). We denote the last \( n \) rows as \( f_1, \ldots, f_n \).

As in Lemma 1.3, \( \nabla_x x \) is a \( K \)-linear combination of \( \nabla_y y, f_1, \ldots, f_n \). That is,
\[
\nabla_x x = d\nabla_y y + d_1f_1 + \cdots + d_nf_n,
\]
where \( d, d_1, \ldots, d_n \) are elements of \( K \). The \( i \)th column of the Jacobian implies \( (x)_{x_i} = d_i y_i \) and hence \( d_i = (x)_{x_i}/y_i \). The \( (n+i) \)th column of the Jacobian implies \( 0 = d(y)_{y_i} + ((x)_{x_i}/y_i)x_i \). So \( (x)_{x_i} = -d(y/x_i)(y)_{y_i} \).

Assume \( n > 1 \). So
\[
r^2 = \frac{(x)_{x_2}}{(x)_{x_1}} = \frac{y_2/x_2(y)_{y_2}}{y_1/(x)_{y_1}} = -\frac{x_1y_2}{y_1x_2y_1}.
\]
As \( r^2 \neq 0 \), \( x_1y_2 + x_2y_1 = 0 \). Thus, \( x_1, x_2, y_1, \) and \( y_2 \) are algebraically dependent, which is a contradiction. This completes the proof of Proposition 1.1  □
Henceforth in Section 1 we omit the details of linear algebra arguments similar to those above.

Using the formula $\text{Id}(u, v)$ we can encode quantification over $I$ by coding $I$ as $I^*_I = \{u : L(u)\}$ where $L(u)$ is $(\exists v)\text{Id}(u, v)$. $I$ can also be encoded as $I^*_n = \{v : R(v)\}$ where $R(v)$ is $(\exists u)\text{Id}(u, v)$. The formula $\text{Id}(u, v)$ gives a one-to-one correspondence between $I^*_I$ and $I^*_n$. We now discuss how to encode quantification over all functions from $I$ to $I$.

Let $f$ be a function from $I$ to $I$. Let $K_f^* = (x_{f(i)} + y_i : i \in I)$. $K_f^*$ encodes $f$ viewed as a function from $I^*_I$ to $I^*_I$. In more detail: Let $F_f(u, v)$ be the following formula with parameter $K_f^*$:

$$L(u) \& L(v) \& (\exists w)(\text{Id}(u, w) \& ((v \text{ join } w) \text{ meet } K_f^* \text{ is one dimensional})$$

**Proposition 1.4.** $f(i) = j$ if and only if $(x_j, y_i)$ meet $K_f^*$ is one dimensional.

**Proof.** By Proposition 1.1, $\text{Id}((x_i), w)$ if and only if $w = (y_i)$. So it suffices to show that $f(i) = j$ if and only if $(x_j, y_i)$ meet $K_f^*$ is one dimensional.

Assume $f(i) = j$. So $x_j + y_i \in (x_j, y_i)$ meet $K_f^*$, and hence $(x_j, y_i)$ meet $K_f^*$ has dimension at least 1. If the dimension is greater than 1, then $y_i$ is in $K_f^*$. With relabeling we may assume that $i = 1$ and that $y_i \in (x_{f(1)} + y_1, \ldots, x_{f(m)} + y_n)$, where $f(1), \ldots, f(m)$ are distinct and $f(k) \in \{f(1), \ldots, f(m)\}$ for $k = m + 1, \ldots, n$. Hence,

$$J(y_1, x_{f(1)} + y_1, \ldots, x_{f(n)} + y_n; x_{f(1)}, \ldots, x_{f(m)}, y_1, \ldots, y_n)$$

has rank $n$. By linear algebra this is impossible.

Now assume $(x_j, y_i)$ meet $K_f^*$ is one dimensional. Say it is $(z)$. By relabeling we may assume that

(a) $z \in (x_{f(1)} + y_1, \ldots, x_{f(n)} + y_n)$,
(b) $j \in \{f(1), \ldots, f(n)\}$ and $i = 1$,
(c) $f(1), \ldots, f(m)$ are distinct and $f(k) \in \{f(1), \ldots, f(m)\}$ for $k = m + 1, \ldots, n$.

As $(x_j, y_i)$ meet $(x_{f(1)} + y_1, \ldots, x_{f(n)} + y_n)$ is one dimensional, $x_j, y_i, x_{f(1)} + y_1, \ldots, x_{f(n)} + y_n$ are algebraically dependent. Hence

$$J(x_j, y_1, x_{f(1)} + y_1, \ldots, x_{f(n)} + y_n; x_{f(1)}, \ldots, x_{f(m)}, y_1, \ldots, y_n)$$

has rank at most $n + 1$. Linear algebra shows this only occurs if $j = f(1)$. □

To quantify over functions from $I$ to $I$ we can not just quantify over the $K_f^*$'s as in the lattice $\mathcal{L}_n^*$ we can not define the sums used in the definitions of the $K_f^*$'s.

Instead we proceed as follows:

We say $K^*$ encodes a function from $I$ to $I$ if

$$(\forall u)_{R(u)}(\exists! u)_{I \cup \omega}((u \text{ join } v) \text{ meet } K^* \text{ is one dimensional}).$$
By Proposition 1.4, \( f \) is encoded by \( K_f^* \). In fact, \( f \) is also encoded by many other members of the lattice. Using any \( K^* \) encoding \( f \) we can define the action \( f' \) of \( f \) on \( I_f^* \) by:

\[
f'(u) = v \quad \text{iff} \quad L(u) \& L(v) \& (\exists w)(\text{Id}(u, w) \& (v \text{ join } w) \text{ meet } K^* \text{ is one dimensional}).
\]

We, thus, can encode quantification over all functions from \( I \) to \( I \). This proves:

**Theorem 1.5.** *In the first-order theory of \( \mathcal{L}^* \) one can encode all formulae with quantification over elements of \( I \) and with quantification over functions from \( I \) to \( I \). Hence the first-order theory of \( \mathcal{L}^* \) has the logical complexity of full second-order logic on \( I \).*

**Notation.** Given any formula \( \Phi \) of full second-order logic we let \( \Phi^*(K_x^*, K_y^*, K_p^*, K_t^*) \) be the translation sketched above of \( \Phi \) into the first-order language of the lattice \( \mathcal{L}^* \).

It remains to eliminate the use of the parameters \( K_x^*, K_y^*, K_p^*, \) and \( K_t^* \). The crucial idea in doing this is that we only used certain syntactic properties of the one-to-one correspondence given by \( \text{Id} \). Roughly speaking we say that parameters are nice if they allow us to obtain such a one to one correspondence. More precisely:

Let \( \text{Id}(u, v, K_x, K_y, K_p, K_t) \) be the formula

\[
\begin{align*}
(\text{ia}) \quad & u \text{ is one dimensional contained in } K_x \\
& \& (\text{ib}) \quad v \text{ is one dimensional contained in } K_y \\
& \& (\text{ii}) \quad (u \text{ join } v) \text{ meet } K_p \text{ is one dimensional} \\
& \& (\text{iii}) \quad (u \text{ join } v) \text{ meet } K_t \text{ is one dimensional}.
\end{align*}
\]

We will usually just write \( \text{Id}(u, v, \text{PARAM}) \). Let \( L(u, \text{PARAM}) \) be \( (\exists v) (\text{Id}(u, v, \text{PARAM})) \) and \( R(v, \text{PARAM}) \) be \( (\exists u) (\text{Id}(u, v, \text{PARAM})) \).

We say the quadruple \( (K_x, K_y, K_p, K_t) \) is nice if

\[
\begin{align*}
(\text{a}) \quad & \forall u, v, v' (\text{Id}(u, v, \text{PARAM}) \& \text{Id}(u, v', \text{PARAM}) \rightarrow v = v') \\
& \& (\forall u, u', v (\text{Id}(u, v, \text{PARAM}) \& \text{Id}(u', v, \text{PARAM}) \rightarrow u = u') \\
& \& (K_x \text{ join } K_y = K) \\
& \& (\forall K'_x (K'_x \subseteq K_x \rightarrow (\exists u)(L(u, \text{PARAM}) \& u \notin K'_x))) \\
& \& (\forall K'_y (K'_y \subseteq K_y \rightarrow (\exists v)(R(v, \text{PARAM}) \& v \notin K'_y))) \\
& \& (K_x \text{ meet } K_y = k) \\
& \& (\forall u)_{L(u, \text{PARAM})} (\exists K' \subseteq K) ((\forall u')(\exists u' \subseteq K') (u' \neq u \rightarrow u' \subseteq K')) \\
& \& (\forall u)_{R(v, \text{PARAM})} (\exists K' \subseteq K) ((\forall u')(\exists v' \subseteq K') (v' \neq v \rightarrow v' \subseteq K')) \\
& \& (\forall u)_{L(u, \text{PARAM})}(u \subseteq K') \\
& \& (\forall u)_{R(v, \text{PARAM})}(v \subseteq K') \\
& \& (\forall u)_{L(u, \text{PARAM})}(u \subseteq K') \\
& \& (\forall u)_{R(v, \text{PARAM})}(v \subseteq K').
\end{align*}
\]
Claim. \( \text{Id} \) gives a one-to-one correspondence between \( I_L = \{u : L(u, \text{PARAM})\} \) and \( I_R = \{v : R(v, \text{PARAM})\} \). And, hence, \( I_L \) and \( I_R \) are equinumerous.

Proof. This is a rephrasing of (a). \( \square \)

Claim. The span of \( I_L \) is \( K_X \) and the span of \( I_R \) is \( K_Y \). And, hence, the span of \( I_L \cup I_R \) is \( K \).

Proof. As \( u \in I_L \rightarrow u \subseteq K_X \), the span of \( I_L \) is contained in \( K_X \). Let \( K'_X = \text{span}(I_L) \). If \( K'_X \subseteq K_X \), then by (b) there is a \( u \) in \( I_L \) such that \( u \notin K'_X \). This contradicts the definition of \( K'_X \). \( \square \)

Claim. \( I_L \) and \( I_R \) are disjoint.

Proof. This is an immediate consequence of (c). \( \square \)

Claim. \( I_L \cup I_R \) is a basis of \( K \).

Proof. If not, then either there is a \( u \) in \( I_L \) which is in \( \text{cl}(I_L - \{u\}) \cup I_R \) or there is a \( v \) in \( I_R \) which is in \( \text{cl}(I_L \cup (I_R - \{v\})) \). As \( I_L \cup I_R \) spans \( K \), both of these are are precluded by (d). \( \square \)

Proposition 1.1 shows that \( \langle K^*_X, K^*_Y, K^*_P, K^*_T \rangle \) is a nice quadruple. Given any nice quadruple we can encode quantification over a set of cardinality \( K \)—specifically over the set \( I_L \), and we can encode quantification over functions from \( I_L \) to \( I_L \), just as we did in the proof of Theorem 1.5 for quantification over \( I^*_L \) and for quantification over functions from \( I^*_L \) to \( I^*_L \). Thus, we can interpret a second-order formula \( \Phi \) as the first-order formula

\[
(\forall K_X, K_Y, K_P, K_T)(\langle K_X, K_Y, K_P, K_T \rangle \text{ is nice} \rightarrow \Phi^*(K_X, K_Y, K_P, K_T))
\]

We have, thus, proven:

**Theorem 1.6.** In the first-order theory of \( \mathcal{L} \) one can encode all formulae with quantification over elements of \( I \) and with quantification over functions from \( I \) to \( I \). Hence the first-order theory of \( \mathcal{L} \) has the logical complexity of full second-order logic on \( I \).

Similar arguments may be given for the lattice \( \mathcal{L} \) of subspaces of a vector space \( V \) over a field \( F \).

**Theorem 1.7.** The first-order theory of \( \mathcal{L} \) has logical complexity at least that of second-order logic on a set of cardinality \( = \text{min} (\text{dim}_F(V), \text{card}(F)) \).

**Sketch of proof.** We continue to let \( (w_j : j \in J) \) denote \( \text{cl}(\{w_j : j \in J\}) \), but here \( \text{cl} \) is ‘linear span’.

The characterization of transcendence degree is replaced by the well known similar characterization of linear dimension. This is:
Some highly undecidable lattices

If \( x_1, \ldots, x_n \) are linearly independent and \( u_1, \ldots, u_m \in (x_1, \ldots, x_n) \), then the \( F \)-dimension of \((u_1, \ldots, u_m)\) is the rank of the coordinate matrix

\[
(a_{ij})_{i=1, \ldots, n \text{ and } j=1, \ldots, m}
\]

where \( a_{ij} \) are the coordinates of \( u_j \) with respect to \( x_1, \ldots, x_n \). (That is, \( u_j = a_{j1}x_1 + \cdots + a_{jn}x_n \).)

As in the proof of Theorems 1.5 and 1.6 one splits a vector space basis \( B \) of \( V \) into two disjoint subsets \( B_X = \{x_i: i \in I\} \) and \( B_Y = \{y_i: i \in I\} \). We use these to form similar parameters as before—namely \( V_X = (B_X), \ V_Y = (B_Y), \ V_T = (x_i + y_i: i \in I) \) and \( V_F = (x_i + b_i y_i: i \in I) \) where \( \langle b_i: i \in I \rangle \) is a sequence of distinct elements of \( F \). It is the use of this sequence which leads to the factor of \( \text{card}(F) \) in the statement of Theorem 1.7. All remaining details of the proof are left to the reader. \( \square \)

The only cases of Theorem 1.7 not covered by the results of Section 2 are when both \( F \) and \( \text{dim}_F(V) \) are uncountable.

**Section 2**

Let \( S \) be a nontrivial Steinitz Exchange System of infinite dimension over \( \text{cl}(\emptyset) \).

As in Section 1 we let \((w_j: j \in J)\) denote \( \text{cl}(\{w_j: j \in J\}) \).

Let \( Q \) be a subset of \( S \).

**Definition.** \( \text{cl}_Q(R) = \text{cl}(Q \cup R) \).

\( (S, \text{cl}_Q) \) is also a Steinitz Exchange System. We say a set is \( Q \)-independent if it is independent with respect to \( \text{cl}_Q \).

We let \( Q(w_j: j \in J) \) denote \( \text{cl}_Q(\{w_j: j \in J\}) \).

**Definition.** \( w \) depends on \( w_1, \ldots, w_n \) if \( w_1, \ldots, w_n \) are independent, \( w \in (w_1, \ldots, w_n) \), and for \( i = 1, \ldots, n \) \( w_i \in (w_1, \ldots, w_n) \) with \( w_i \) replaced by \( w \).

Similarly we define \( w \) \( Q \)-depends on \( w_1, \ldots, w_n \).

**Definition.** Let \( B = \{x_i: i \in I\} \) be a basis of \( X \). Let \( u \in X \). It is easy to see that there are unique \( i_1, \ldots, i_n \in I \) such that \( u \) depends on \( x_{i_1}, \ldots, x_{i_n} \). Let \( B\text{-support}(u) = \{x_{i_1}, \ldots, x_{i_n}\} \).

Say \( w \) is one dimensional and that \( w = (b) \). We frequently write \( w \) in place of \( b \), and vice versa.

We often use the following elementary facts without mention.

**Lemma 2.1.** (a) If \( I = \{x_{ij}: 1 \leq i \leq m \text{ and } 1 \leq j \leq n_i\} \) is independent; for \( 1 \leq i \leq m \), \( x_i \) depends on \( x_{i1}, \ldots, x_{in_i} \); and \( x \) depends on \( x_1, \ldots, x_n \); then \( x \) depends on \( I \).

(b) If \( x_1, \ldots, x_n \) are independent, then there is an \( x \) which depends on \( x_1, \ldots, x_n \).
Proof. Left to the reader. □

Let $\mathcal{L}$ be the lattice of cl-closed subsets of $S$. Let $\mathcal{L}^*$ consist of $\mathcal{L}$ together with several parameters to be defined later. As in Section 1 we first show that $\mathcal{L}^*$ has logical complexity at least that of second-order number theory, and we then show how to eliminate the use of these parameters.

We begin with some preliminary work on coding functions.

Definition (in $\mathcal{L}$). $X$ and $Y$ are independent if $X' \subseteq X$ and $Y' \subseteq Y$ and $X'$ join $Y' = X$ join $Y$ implies $X' = X$ and $Y' = Y$.

Notation (in $\mathcal{L}$). $u \subseteq Z$ if $u$ is one dimensional and $u \subseteq Z$.

Definition (in $\mathcal{L}$). Let $X$ and $Y$ be independent, with $\dim(X) = \dim(Y)$. $A$ is a precode of a function from $X$ onto $Y$ if $u \subseteq X$ and $v \subseteq Y$ implies $(u \join v) \meet A$ has dimension 0 or 1.

Notations. Say $A$ is a precode of a function from $X$ onto $Y$.

$G(A) =$ the graph of $A$

$$= \{(u, v) : u \subseteq X, v \subseteq Y \text{ and } \dim((u \join v) \meet A) = 1\},$$

$\Dom(A) = \{u : \exists v \langle u, v \rangle \in G(A)\}$,

$\Rng(A) = \{v : \exists u \langle u, v \rangle \in G(A)\}$.

For $X_1 \subseteq X$, $u \subseteq A, 1 \subseteq X_1$ if $u \subseteq X_1$ and $u \in \Dom(A)$.

For $Y_1 \subseteq Y$, $v \subseteq A, 1 \subseteq Y_1$ if $v \subseteq Y_1$ and $v \in \Rng(A)$.

$X_1$ is $\Dom(A)$-spanned

if $X_1 \subseteq X$ and $\neg(\exists X_2 \subseteq X_1)(\forall u)(u \subseteq A, 1 \subseteq X_1 \rightarrow u \subseteq X_2)$.

$Y_1$ is $\Rng(A)$-spanned

if $Y_1 \subseteq Y$ and $\neg(\exists Y_2 \subseteq Y_1)(\forall v)(v \subseteq A, 1 \subseteq Y_1 \rightarrow v \subseteq Y_2)$.

Definition (in $\mathcal{L}$). Let $X$ and $Y$ be independent with $\dim(X) = \dim(Y)$. $A$ is a weak code of a function from $X$ onto $Y$ if

1. $G(A)$ is a 1-1, onto function from $\Dom(A)$ to $\Rng(A)$,
2. $X$ is $\Dom(A)$-spanned and $Y$ is $\Rng(A)$-spanned, and
3. $G(A)$ is dependency preserving, that is (a) and (b) below hold.

Notations. If $\langle u, v \rangle \in G(A)$, then $A(u) = v$ and

$A\text{-code}(u, v) = (u \join v) \meet A$.

If $X_1$ is $\Dom(A)$-spanned, then $A[X_1] = (A(u) : u \subseteq A, 1 \subseteq X_1)$.

If $Y_1$ is $\Rng(A)$-spanned, then $A^{-1}[Y_1] = (u : A(u) \subseteq A, 1 \subseteq Y_1)$.
Some highly undecidable lattices

(a) If for i = 1, 2, \(X_i \subseteq X\), \(X_i\) is \(\text{Dom}(A)\)-spanned, \(Y_i = A[X_i]\), and \(X_1\) and \(X_2\) are independent; then \(Y_1\) and \(Y_2\) are independent and \(Y_1 \Join Y_2 = A[X_1 \Join X_2]\).

(b) If for i = 1, 2, \(Y_i \subseteq Y\), \(Y_i\) is \(\text{Rng}(A)\)-spanned, \(X_i = A^{-1}[Y_i]\), and \(Y_1\) and \(Y_2\) are independent; then \(X_1\) and \(X_2\) are independent and \(X_1 \Join X_2 = A^{-1}[Y_1 \Join Y_2]\).

It is appropriate to call condition (3) above 'dependency preserving' as:

**Proposition 2.2.** Assume (1) and (2) of the definition of "\(A\) is a weak code of a function from \(X\) onto \(Y\)" hold. Then the following are equivalent:

(3) As above.

(4) For any \(S \subseteq \text{Dom}(A)\), \(S\) is independent if and only if \(\{A(u) : u \in S\}\) is independent.

(5) For any finite \(S \subseteq \text{Dom}(A)\), \(S\) is independent if and only if \(\{A(u) : u \in S\}\) is independent.

**Proof.** Assume (3). Let \(S = \{u_1, \ldots, u_n\} \subseteq \text{Dom}(a)\). Assume \(S\) is independent. We prove by induction on \(k\) that

\[
(*) \quad A(u_1), \ldots, A(u_k) \text{ are independent and } A[(u_1, \ldots, u_k)] \text{ has dimension } k \text{ and hence is } (A(u_1), \ldots, A(u_k)).
\]

For \(k = 1\) \((*)\) is trivial. Assume \((*)\) for \(k\).

Let \(X_1 = (u_1, \ldots, u_k)\) and \(X_2 = (u_{k+1})\). By induction \(A(u_1), \ldots, A(u_k)\) are independent and \(Y_1 = A[X_1]\) has dimension \(k\). Let \(Y_2 = A(u_{k+1})\). By (3a) \(Y_1\) and \(Y_2\) are independent.

Hence, \(A(u_1), \ldots, A(u_{k+1})\) are independent and \(Y_1 \Join Y_2\) has dimension \(k + 1\). Also by (3a), \(Y_1 \Join Y_2 = A[(u_1, \ldots, u_{k+1})]\).

Similarly \(\{A(u) : u \in S\}\) is independent implies \(S\) is independent.

Thus, (3) implies (5).

It is easy to show that (5) implies (4).

Assume (4). We prove (3a). The proof of (3b) is similar.

Let \(X_i\) and \(Y_i\) be as in the hypotheses of (3a). As \(X_i\) is \(\text{Dom}(A)\)-spanned, \(X_i\) has a basis \(B_i\) which is contained in \(\text{Dom}(A)\). As \(X_1\) and \(X_2\) are independent, \(B_1\) and \(B_2\) are disjoint and \(B_1 \cup B_2\) is independent. So by (4), \(\{A(u) : u \in B_1 \cup B_2\}\) is independent.

**Claim.** If \(v\) is \(A, 1 \subseteq X_1\), then \(A(v) \subseteq (A(u) : u \in B_1)\).

**Proof.** As \(v \subseteq X_1\), \(v\) depends on a finite subset \(B'_1\) of \(B_1\). By (4), \(\{A(u) : u \in B'_1\}\) is independent. Also by (4), \(\{A(v)\} \cup \{A(u) : u \in B'_1\}\) is dependent (for if not then \(\{v\} \cup B'_1\) would be independent). Hence \(A(v) \subseteq (A(u) : u \in B'_1)\).

Using the above claim we obtain \(Y_1 = (A(u) : u \in B_1)\).

Similarly \(Y_2 = (A(u) : u \in B_2)\) and \(A[X_1 \Join X_2] = (A(u) : u \in B_1 \cup B_2)\).

Hence the conclusions of (3a) hold. □
Theorem 2.3 (Basic Existence Theorem). Let $X$ and $Y$ be independent with \( \dim(X) = \dim(Y) \).

If $B_X = \{x_i : i \in I\}$ is a basis of $X$ and $B_Y = \{y_i : i \in I\}$ is a basis of $Y$, then there is a weak code $A$ of a function from $X$ onto $Y$ such that $G(A)$ contains \( \{((x_i), (y_i)) : i \in I\} \).

We call such an $A$ a weak code of the function which sends $x_i$ to $y_i$ for $i \in I$.

**Proof.** For each $i \in I$ let $a_i$ (also denoted $a(x_i, y_i)$) depend on $x_i$ and $y_i$. Let $A = \{a_i : i \in I\}$ and $B_A = \{a_i : i \in I\}$. We show $A$ is a weak code of a function from $X$ onto $Y$. It is easy to show that $A$ is a precede of a function from $X$ onto $Y$, and that $G(A)$ contains \( \{((x_i), (y_i)) : i \in I\} \).

Although we have not yet proven that $G(A)$ is a function from $\Dom(A)$ to $\Rng(A)$, if $\langle u, v \rangle \in G(A)$, then we abusively write $A(u) = v$ and $A$-code($u, v$) = ($u$ join $v$) meet $A$.

**Remarks.** (1) A simple example of such an $A$ occurs in Section 1 with $X = K^*_X$, $Y = K^*_Y$, and $A = K^*_S$. Proposition 2.4 below shows that the dependency preserving properties of $K^*_p$, which were proven in Lemma 1.3 using Jacobians, can be proven just using the axioms of a Steinitz Exchange System.

(2) We call such codes $A$ 'weak codes' as \( \{((x_i), (y_i)) : i \in I\} \) may be a proper subset of $G(A)$.

2.4 through 2.7 below concern the setting of the proof of Theorem 2.3.

**Proposition 2.4.** $A$ is dependency preserving. In fact, for $i \in J$ let $u_i \in \Dom(A)$, let $v_i = A(u_i)$, and let $b_i = A$-code($u_i, v_i$). Then the following are equivalent:

1. $\{u_i : i \in J\}$ is independent.
2. $\{v_i : i \in J\}$ is independent.
3. $\{b_i : i \in J\}$ is independent.

**Proof.** Deferred.

**Corollary 2.5.** For $i = 1, \ldots, n$ let $u_i \in \Dom(A)$, let $v_i = A(u_i)$, and let $b_i = A$-code($u_i, v_i$). Assume $u_1, \ldots, u_n$ are independent. Let $u \in \Dom(A)$, let $v = A(u)$, and let $b = A$-code($u, v$). The following are equivalent:

1. $u$ depends on $u_1, \ldots, u_n$.
2. $v$ depends on $v_1, \ldots, v_n$.
3. $b$ depends on $b_1, \ldots, b_n$.

**Proof.** Assume $u_1, \ldots, u_n$ are independent. By Proposition 2.4 $v_1, \ldots, v_n$ are independent and $b_1, \ldots, b_n$ are independent.
Assume (1) of Corollary 2.5. So \( \{u_i: 1 \leq i \leq n\} \) is dependent and \( \{u_i: 1 \leq i \leq n \text{ except for } i = k\} \) is independent for \( 1 \leq k \leq n \). By (1) implies (2) of Proposition 2.4, \( \{v\} \cup \{v_i: 1 \leq i \leq n\} \) is dependent. And by (2) implies (1) of Proposition 2.4, \( \{v\} \cup \{v_i: 1 \leq i \leq n \text{ except for } i = k\} \) is independent for \( 1 \leq k \leq n \). Hence (2) of Corollary 2.5 holds.

Similarly (2) implies (3) and (3) implies (1).

**Corollary 2.6.** For \( i \in I \) let \( u_i \in \text{Dom}(A) \), let \( v_i = A(u_i) \), and let \( b_i = A\text{-code}(u_i, v_i) \).

The following are equivalent:

1. \( \{u_i: i \in I\} \) is a basis of \( X \).
2. \( \{v_i: i \in I\} \) is a basis of \( Y \).
3. \( \{b_i: i \in I\} \) is a basis of \( A \).

**Proof.** Assume (1) of Corollary 2.6. By Proposition 2.4, \( \{v_i: i \in I\} \) is independent. Let \( V = \{v_i: i \in I\} \). It suffices to show \( y_j \in V \) for every \( j \in I \). As \( \{u_i: i \in I\} \) is a basis of \( X \), \( x_j \) depends on a finite number of \( u_i \)'s. By Corollary 2.5, \( y_j \) depends on a finite number of \( v_i \)'s and hence is contained in \( V \).

Similarly (2) implies (3) and (3) implies (1).

**Proof of Theorem 2.3** (completed). It remains to show \( G(A) \) is 1–1 and a function from \( \text{Dom}(A) \) onto \( \text{Rng}(A) \). These are immediate consequences of Corollary 2.5 in the special case \( n = 1 \).

For the proof of Proposition 2.4 we need the following lemma:

**Lemma 2.7.** Corollary 2.5 holds in the special case that \( u_k = (x_n) \) and \( v_k = (y_n) \) for \( k = 1, \ldots, n \) where \( i_1, \ldots, i_n \) are distinct members of \( I \).

**Proof.** We first prove (1) is equivalent to (2).

We leave it to the reader to show that \( \{u\} \cup \{a_i: i \in I\} \) is independent, and that similarly \( \{v\} \cup \{a_i: i \in I\} \) is independent.

On the other hand as \( (u \text{ join } v) \) meet \( A \) is one dimensional, \( \{u, v\} \cup \{a_i: i \in I\} \) is dependent.

Assume \( u \) and \( v \) do not depend on the same \( x_i \)'s and \( y_j \)'s respectively. By relabeling elements of \( I \) and perhaps exchanging \( u \) and \( v \) we may assume:

- \( u \) depends on \( x_1, \ldots, x_n \);
- \( v \) depends on \( y_1, \ldots, y_m, y_{n+1}, \ldots, y_p \) where \( m < n \) and \( p \geq n \).

One may easily conclude \( u, v, a_1, \ldots, a_p \) are dependent. Let

\[ Z = \{y_k: 1 \leq k \leq p \text{ except for } k = n\} \cup \{a_k: 1 \leq k \leq p\} \]

Let \( T = \text{cl}(Z) \). We show our assumption is wrong by showing that \( T \) contains the \( 2p \) independent elements \( x_1, \ldots, x_p, y_1, \ldots, y_p \). This contradicts that the basis \( Z \) of \( T \) consists of \( 2p - 1 \) elements.

\( v \in T \) as \( v \) depends on the elements \( y_1, \ldots, y_m, y_{n+1}, \ldots, y_p \) of \( T \).
For 1 \leq k \leq p except for \( k = n \), \( x_k \in T \) as \( x_k \) depends on the elements \( y_k, a_k \) of \( T \).

\( x_n \in T \) as \( x_n \) depends on the elements \( x_1, \ldots, x_{n-1}, u \) of \( T \).

\( y_n \in T \) as \( y_n \) depends on the elements \( x_n, a_n \) of \( T \).

To prove (2) is equivalent to (3), we apply (1) is equivalent to (2) of Lemma 2.7 in the case where \( X \) is replaced by \( Y \), \( Y \) is replaced by \( A \) and \( A \) is replaced by \( X \). Lemma 2.7 applies in this case as \( u = (v \Join b) \Meet X \), \( x_i \) depends on \( a_i \) and \( y_i \) for \( i \in I \), \( Y \) and \( A \) are independent, \( B_Y \) is a basis of \( Y \), \( B_A \) is a basis of \( A \), and \( \dim(Y) = \dim(A) \).

Proof of Proposition 2.4. By reasoning similar to that in the proof of Lemma 2.7 it suffices to prove (1) implies (2).

Assume \( \{u_i : i \in J\} \) is independent. We may assume that \( J \subseteq I \) and that \( \{u_i : i \in J\} \) can be extended to a basis \( \{u_i : i \in I\} \) of \( X \) with \( u_i \in \Dom_A \) for all \( i \in I - J \). Also for \( i \in I - J \) let \( v_i = A(u_i) \) and let \( b_i = A\code(u_i, v_i) \).

We show \( \{v_i : i \in I\} \) is independent. Assume not. So there are \( i_1, \ldots, i_n \) such that \( v_{i_1}, \ldots, v_{i_n} \) are dependent. By rearranging the \( v_i \)'s we may assume \( i_k = k \) for \( k = 1, \ldots, n \). Let \( I_k = I - \{1, \ldots, k\} \). By rearranging the \( x_i \)'s we may assume \( U_k = \{u_i : 1 \leq i \leq k\} \cup \{x_i : i \in I_k\} \) is a basis of \( X \) for \( k = 1, \ldots, n \). We prove by induction on \( k \) that

\[ (*) \quad V_k = \{v_i : 1 \leq i \leq k\} \cup \{y_i : i \in I_k\} \quad \text{is a basis of } Y, \quad \text{and} \quad B_k = \{b_i : 1 \leq i \leq k\} \cup \{a_i : i \in I_k\} \quad \text{is a basis of } A. \]

\( (*) \) is trivial for \( k = 0 \).

Assume \( (*) \) for \( k \). So \( X = (U_k), \ Y = (V_k), \) and \( A = (B_k) \). As \( u_{k+1} \in X - \cl(U_{k+1} - \{u_{k+1}\}), \ u_{k+1} \) depends on \( x_{k+1} \) and some \( u_i \)'s for \( 1 \leq i \leq k \) and some \( x_i \)'s for \( i \in I_{k+1} \). Applying Lemma 2.7 to \( X = (U_k), \ Y = (V_k), \) and \( A = (B_k) \) we obtain that \( v_{k+1} \) depends on \( y_{k+1} \) and some \( v_i \)'s for \( 1 \leq i \leq k \) and some \( y_i \)'s for \( i \in I_{k+1} \). This implies \( V_{k+1} \) is independent and spans \( Y \).

Similarly \( B_{k+1} \) is a basis of \( A \).

\( (*) \) for \( n \) implies \( v_1, \ldots, v_n \) are independent.

Thus, (1) implies (2). \( \square \)

Remark. The statement, "\( A = \{a_i : i \in I\} \) for some \( \{a_i : i \in I\}, \ \{y_i : i \in I\}, \) and \( \{a_i : i \in I\} \) are as in the proof of Theorem 2.3, can be expressed in purely lattice-theoretic terms as follows:

"\( A \) is a minimal weak code of a function from \( X \) onto \( Y \)", that is, \( A \) is a weak code of a function from \( X \) onto \( Y \) and there is no proper subset \( A' \) of \( A \) which is a weak code of a function from \( X \) onto \( Y \).

Proof. Assume \( A \) is a minimal weak code of a function from \( X \) onto \( Y \). Let \( B_X \) be a basis of \( \Dom_A \). Let \( B_Y = \{A(u) : u \in B_X\} \). As \( G(A) \) is dependency preserving,
Some highly undecidable lattices

Let $A' = (\text{code}(u, A(u)) : u \in B_y)$. By Theorem 2.3, $A'$ is a weak code of a function from $X$ onto $Y$ and hence $A = A'$.

Conversely, assume $A = (a(x, y)_i : i \in I)$. By Theorem 2.3, $A$ is a weak code of a function from $X$ onto $Y$. Let $A' \subseteq A$ be a weak code of a function from $X$ onto $Y$. Let $B_U = \{u_i : i \in I\}$ be a basis of $\text{Dom}_{A'}$, and hence of $X$. Let $B_V = \{A'(u_i) : i \in I\}$. Note: $A'(u_i) = A(u_i)$ for $i \in I$. As $G(A')$ is dependency preserving, $B_V$ is a basis of $Y$. Let $A'' = (A'-\text{code}(u_i, A'(u_i)) : i \in I)$. Note: $A'-\text{code}(u_i, A'(u_i)) = A\text{-code}(u_i, A(u_i))$ for $i \in I$. So $A'' \subseteq A'$. By Corollary 2.6, $A'' = A$ and, hence, $A' = A$.  

Remark. One also would like to have weak codes of functions from $X$ onto $Y$ when $X$ and $Y$ are not independent. In the special case that there is a $Z$ such that

1. $X$ and $Z$ have the same dimension,
2. $X$ and $Z$ are independent, and
3. $Z$ and $Y$ are independent,

a weak code of a function from $X$ onto $Y$ may be defined to be an ordered pair $[A, B]$ such that

1. $A$ is a weak code of a function from $X$ onto $Z$,
2. $B$ is a weak code of a function from $Z$ onto $Y$, and
3. $\{u : u \in \text{Dom}_A$ and $A(u) \in \text{Dom}_B\}$ spans $X$.

We abusively use the phrase ‘weak code’ in place of ‘weak’ code.

In the obvious fashion we define: $G([A, B]) = (u); \ \text{Dom}_{[A, B]} = \{u : u \in \text{Dom}_A$ and $A(u) \in \text{Dom}_B\};$ $\text{Rng}_{[A, B]}; u$ is $[A, B]_1; v$ is $[A, B]_2; 1' \subseteq X'; X'$ is $\text{Dom}_{[A, B]}$-spanned; and $Y'$ is $\text{Rng}_{[A, B]}$-spanned (for $X' \subseteq X$ and $Y' \subseteq Y$). For example:

$$\text{Dom}_{[A, B]} = \{u : u \in \text{Dom}_A$ and $A(u) \in \text{Dom}_B\}.$$ 

Corollary 2.8. If $X$, $Z$, and $Y$ are as above, $B_X = \{x_i : i \in I\}$ is a basis of $X$, and $B_Y = \{y_i : i \in I\}$ is a basis of $Y$, then there is a weak code $[A, B]$ of a function from $X$ onto $Y$ such that $G([A, B])$ contains $\{(x_i, y_i) : i \in I\}$.

Such an $[A, B]$ is also called a weak code of the function which sends $x_i$ to $y_i$ for $i \in I$.

Proof. Let $B_Z = \{z_i : i \in I\}$ be a basis of $Z$. Let $A = (a(x_i, z_i) : i \in I)$ and $B = (a(z_i, y_i) : i \in I)$. Now use Theorem 2.3. 

Definition (in $\mathcal{L}$). A weak code of a function from $X$ into $Y$ is a weak code of a function from $X$ onto $Y'$ for some $Y' \subseteq Y$.

Let $P$ be the set of nonnegative integers.
Let $B_{sq} = \{x_{i,j}: i, j \in P\}$ and $B_{sq}' = \{y_{i,j}: i, j \in P\}$ be disjoint so that $B_{sq} \cup B_{sq}'$ is independent. Some of the parameters we will use are:

Square = $(x_{i,j}: i, j \in P) = \left( \begin{array}{cccc} \vdots & \vdots & \vdots & \cdots \\ x_{2,0} & x_{2,1} & x_{2,2} & \cdots \\ x_{1,0} & x_{1,1} & x_{1,2} & \cdots \\ x_{0,0} & x_{0,1} & x_{0,2} & \cdots \end{array} \right)$

Square' = $(y_{i,j}: i, j \in P) = \left( \begin{array}{cccc} \vdots & \vdots & \vdots & \cdots \\ y_{2,0} & y_{2,1} & y_{2,2} & \cdots \\ y_{1,0} & y_{1,1} & y_{1,2} & \cdots \\ y_{0,0} & y_{0,1} & y_{0,2} & \cdots \end{array} \right)$

Row0 = $(x_{0,j}: j \in P), \quad \text{Diag} = (x_{j,j}: j \in P), \quad \text{Col0} = (x_{i,0}: i \in P), \quad \text{Idsq} = (a(x_{i,j}, y_{i,j}): i, j \in P), \quad \text{a weak code of the function from Square onto Square' sending } x_{i,j} \text{ to } y_{i,j} \text{ for all } i, j \in P.$

Using the above parameters we can define other parameters including:

Row0' = $(y_{0,j}: j \in P), \quad \text{Diag'} = (y_{j,j}: j \in P), \quad \text{Col0'} = (y_{i,0}: i \in P), \quad \text{Idsq meet (Row0 join Row0')} \quad \text{IdDiag} = \text{Idsq meet (Diag join Diag')}, \quad \text{IdCol0} = \text{Idsq meet (Col0 join Col0')}, \quad \text{and } (x_{0,0}) = \text{Col0 meet Row0}.$

The remaining parameters consist of:

Proj = $(a(y_{0,j}, x_{j,j}): j \in P)$

(Proj' = [IdRow0, Proj] is a weak code of the projection map from Row0 onto Diag sending $x_{0,j}$ to $x_{j,j}$ for $j \in P$),

VS = $(a(y_{i,j}, x_{i+1,j}): i, j \in P)$

(VS' = [Idsq, VS] is a weak code of the vertical shift map from Square into Square sending $x_{i,j}$ to $x_{i+1,j}$ for $i, j \in P$), and

Refl = $(a(y_{0,j}, x_{j,0}): j \in P)$

(Refl' = [IdRow0, Refl] is a weak code of the reflection map from Row0 onto Col0 sending $x_{0,j}$ to $x_{j,0}$ for $j \in P$).

We abusively denote Proj' as Proj, VS' as VS, and Refl' as Refl.

We denote the sequence of the above parameters as PARAM.

Our next goal is to define $\left((x_{0,j}): j \in P\right)$. We do this by defining the notion of (a weak code for) a nice function $h$ from Col0 to Square and proving that it $h$ is a nice function, then $h((x_{0,j})) = (x_{0,j})$ for some $j \in P$. We adapt a technique of Shelah [4]. Roughly speaking we say that $h$ is nice if (1)–(3) hold:

1. $h((x_{0,j})) \subseteq \text{Row0}$,
(2) \( h((x_0,0)) \in \text{Dom}_{\text{Proj}} \) & \( h((x_0,0)) \in \text{Dom}_{\text{Refl}} \)
& \( \text{Refl}(h((x_0,0))) \in \text{Dom}_h \) & \( \text{Proj}(h((x_0,0))) = h(\text{Refl}(h((x_0,0)))) \)

(3) \( h \) commutes with \( \text{VS} \).

In fact, we can not expect (3) to be true for the weak code \( h' = [\text{Id}_{\text{Colo}}, h_j] \) (where \( h_j = (a(y_i,0, x_{i,j}) : i \in P) \) of the function which sends \( x_{i,0} \) to \( x_{i,j} \) for \( i \in P \). Below we weaken (3) in order to be able to prove \( h' \) is nice. It is instructive first to see why conditions (1), (2) and (3) guarantee that \( h((x_0,0)) = (x_{i,j}) \) for some \( j \in P \).

(1) guarantees that \( h((x_0,0)) \) depends on elements \( x_{0,j_1}, \ldots, x_{0,j_n} \) where \( j_1 < \cdots < j_n \). As \( \text{Proj} \) is dependency preserving, \( \text{Proj}(h((x_0,0))) \) depends on \( x_{j_1,j_1}, \ldots, x_{j_n,j_n} \). Similarly \( \text{Refl}(h((x_0,0))) \) depends on \( x_{j_1,0}, \ldots, x_{j_n,0} \). As \( h \) is dependency preserving, \( x^* = h(\text{Refl}(h((x_0,0)))) \) depends on \( h((x_{j_1,0})), \ldots, h((x_{j_n,0})) \). By (2), \( x^* = \text{Proj}(h((x_0,0))) \). (3) guarantees that \( h((x_i,0)) \) depends on \( x_{j_1,0}, \ldots, x_{j_n,0} \). Hence by Proposition 2.1, \( x^* \) depends on \( x_{j_1,j_1}, \ldots, x_{j_n,j_n} \). We handle the difficulties with (3) by arranging instead:

(3') \( \text{Sq-sup} \) support \( (h(x^*)) \) is \( \text{Row}_{j_n} \) correct, that is, it consists of \( x_{j_1,j_1}, \ldots, x_{j_n,j_n} \), together with possibly some elements \( x_{i,j} \) for \( i < j \) (where \( j_1, \ldots, j_n \) are as above). This still gives a contradiction unless \( n = 1 \).

We handle the difficulties with (3) by arranging instead:

(3') \( \text{Sq-support} \) \( (h(x^*)) \) is \( \text{Row}_{j_n} \) correct, that is, it consists of \( x_{j_1,j_1}, \ldots, x_{j_n,j_n} \), together with possibly some elements \( x_{i,j} \) for \( i < j \) (where \( j_1, \ldots, j_n \) are as above). This still gives a contradiction unless \( n = 1 \).

**Lemma 2.9.** The following statements are expressible in the first-order theory of \( \mathfrak{L} \):

(a) \( I \) is infinite dimensional.
(b) \( I \) has countably infinite dimension.

**Proof.** We say \( I \) is small if there is a \( J \) independent of \( I \) with \( \dim(J) \geq \dim(I) \). As we have only defined weak codes of functions from \( I \) into \( I \) when \( I \) is small, the lattice-theoretic characterizations of (a) and (b) are simpler in this case.

For \( I \) small, \( I \) is infinite dimensional if and only if there is a weak code of a function from \( I \) onto a proper subset of \( I \).

For \( I \) small, \( I \) has countably infinite dimension if and only if \( I \) is infinite dimensional and for every infinite dimensional \( J \) contained in \( I \) there is a weak code of a function from \( I \) onto \( J \).

In general, \( I \) is infinite dimensional if there are \( J, K \) contained in \( I \) such that

(1) \( J \) and \( K \) are independent,
(2) there is a weak code of a function from \( J \) into \( K \), and
(3) there is a weak code of a function from \( K \) onto a proper subset of \( J \).

In general, \( I \) has countably infinite dimension if \( I \) has infinite dimension and there are \( J, K \) contained in \( I \) such that

(1) \( J \) and \( K \) are independent,
(2) there is a weak code of a function from \( J \) onto \( K \), and
(3) for any infinite dimensional \( L \) contained in \( J \) there is a weak code of a function from \( J \) onto \( L \). □

**Lemma 2.10.** The following statement is expressible in the first-order theory of \( \mathfrak{L}^* \):
I is an initial segment of Col₀, that is

\[ I = (x_{0,0}, \ldots, x_{n,0}) \text{ for some } n \geq 0. \]

**Proof.**

**Claim.** I is an initial segment of Col₀ if and only if

1. \( (x_{0,0}) \subseteq I, \)
2. I is finite dimensional and contained in Col₀,
3. I is \( \text{Dom}_{\text{vs}} \)-spanned, and
4. \( \exists v \text{ 1-dimensional} \) \( \text{VS}[I] \subseteq I \text{ join } v. \)

It is easy to verify that if I is an initial segment of Col₀, then (1) through (4) hold.

Assume (1) through (4) hold and I is not an initial segment. So there is an integer \( n \) and elements \( (w_1), \ldots, (w_m) \) of \( \text{Dom}_{\text{vs}} \) such that \( x_{0,0}, \ldots, x_{n,0} \in I, \)
\( x_{n+1,0} \notin I \) and \( \{x_{0,0}, \ldots, x_{n,0}, w_1, \ldots, w_m\} \) is a basis of I for some \( m \geq 1. \) Let \( B = \{x_{p,0} : p \in P\}. \) For each \( i, \) \( B \)-support \( (w_i) \) includes \( x_{p,0} \) for some \( p > n. \) Let \( p^* \) be the maximum such \( p \) for all \( i. \) We may assume \( p^* \) occurs for \( w_i. \) By (4) and as VS is dependency preserving, \( \text{VS}[I] = (x_{1,0}, \ldots, x_{n+1,0}, \text{VS}(w_1), \ldots, \text{VS}(w_m)) \) is contained in \( I \) join \( v. \) As \( x_{p^*+1,0} \in B \)-support(\( \text{VS}(w_i) \)) and \( I \subseteq (x_{0,0}, \ldots, x_{p^*,0}) \), we have \( x_{p^*+1,0} \notin B \)-support(\( v \)). So \( v \notin I. \) Also \( x_{n+1,0} \in (I \text{ join } v) - I. \) Hence by the exchange property, \( v \in (x_{0,0}, \ldots, x_{n+1,0}, w_1, \ldots, w_m) \subseteq (x_{0,0}, \ldots, x_{p^*,0}). \) Thus, \( x_{p^*+1,0} \notin B \)-support(\( \text{VS}(v) \)), which gives a contradiction.  \( \square \)

**Definition (in \( L \)).** \( h \) is a nice function from Col₀ into Square if (1)-(3) hold:

1. \( (x_{0,0}) \in \text{Dom}_h \text{ & } h((x_{0,0})) \subseteq \text{Row}_0, \)
2. \( h((x_{0,0})) \in \text{Dom}_{\text{proj}} \text{ & } h((x_{0,0})) \in \text{Dom}_{\text{refl}} \) \( \text{&} \) \( \text{Refl}(h((x_{0,0}))) = \text{Dom}_h \text{ & } \text{Proj}(h((x_{0,0}))) = h(\text{Refl}(h((x_{0,0}))) \text{),} \)
3. For every initial segment I of Col₀, VS and h commute on a basis of I, that is, I is spanned by

\( \{u : u \text{ VS, } 1 \subseteq I \text{ & } u \in \text{Dom}_h \text{ & } \text{VS}(u) \in \text{Dom}_h \text{ & } h(u) \in \text{Dom}_{\text{vs}} \text{ & } \text{VS}(h(u)) = h(\text{VS}(u))\}. \)

**Proposition 2.11.** The following may be expressed by a first-order formula with parameters from \( L^* \):

(a) \( u = (x_{0,j}) \) for some \( j \in P. \)
(b) \( v = (y_{0,j}) \) for some \( j \in P. \)

(We write these formulae as \( P(u, \text{PARAM}) \text{ and } P'(v, \text{PARAM}) \) respectively.)

**Proof of (a).** We show \( u = (x_{0,j}) \) for some \( j \in P \) if and only if there is a nice function \( h \) from Col₀ into Square with \( h((x_{0,0})) = u. \)

First observe that \( h'_j \) (as defined above) is a nice function with \( h'_j((x_{0,0})) = (x_{0,j}). \)
Conversely let \( h \) be a nice function from \( \text{Col}0 \) into \( \text{Square} \). We show \( h((x_{0,0})) = (x_{*,j}) \) for some \( j \in P \).

By (1) there are \( j_1 < \cdots < j_n \) such that \( h((x_{0,j_1})) \) depends on \( x_{0,j_1}, \ldots, x_{0,j_n} \). Let \( x^* = h(\text{Refl}(h((x_{0,0})))) \). By (2), \( x^* = \text{Proj}(h((x_{0,0}))) \). So \( x^* \) depends on \( x_{j_1,1}, \ldots, x_{j_n,n} \). If \( n > 1 \), we obtain a contradiction by showing that \( x_{j_1,1}, \ldots, x_{j_n,n} \in B_{\text{sq}}\text{-support}(x^*) \).

For \( k \geq 0 \), let \( B_k = \{ x_{k,i} : i \in P \} \) and let \( B_k^* = \bigcup \{ B_j : j \leq k \} \).

Claim. There are elements \( x_0^*, x_1^*, \ldots \) of \( \text{Col}0 \) such that for \( k > 0 \)

(a) \( \{ x_0^*, \ldots, x_k^* \} \) is a basis of \( I_k = (x_{0,0}, \ldots, x_{k,0}) \),

(b) \( x_k^* \in \text{Dom}_n \) and \( h((x_k^*)) \) is \( \text{Row} \ k \) correct, that is, \( B_{\text{sq}}\text{-support}(h((x_k^*))) \subseteq B_k^* \) and \( B_{\text{sq}}\text{-support}(h((x_k^*))) \cap B_k = \{ x_{k,j_1}, \ldots, x_{k,j_n} \} \).

We call such a basis of \( I_k \) a special basis and denote it \( B_k^* \).

Proof. For \( k = 0 \), let \( x_0^* = x_{0,0} \).

Assume \( B_k^* = \{ x_0^*, \ldots, x_k^* \} \) is a special basis of \( I_k \). By (3), \( I_k \) has a basis \( B \) on which \( h \) and VS commute. So \( x_k^* \) depends on a subset \( B_\delta \) of \( B \). There is an \( x \in B_\delta \) such that \( \{ x, x_0^*, \ldots, x_{k-1}^* \} \) is independent. (For if not, then \( B_\delta \) and hence \( x_k^* \) are contained in \( \{ x_0^*, \ldots, x_{k-1}^* \} \).) So as \( x \in (x_0^*, \ldots, x_k^*) \), \( x_k^* \in B_{\text{sq}}\text{-support}(x) \). So there are \( i_1, \ldots, i_m < k \) such that \( B_k^*\text{-support}(x) = \{ x_{i_1}^*, \ldots, x_{i_m}^*, x_k^* \} \). So \( h((x)) \) depends on \( h((x_{i_1}^*)), \ldots, h((x_{i_m}^*)), h((x_k^*)) \). Hence, as \( B_k^* \) is a special basis, \( h((x)) \) is \( \text{Row} \ k \) correct. So \( \text{VS}(h((x))) \) is \( \text{Row} \ k + 1 \) correct. Let \( x_{k+1}^* = \text{VS}(x) \). As \( h \) and VS commute on \( (x) \), \( h((x_{k+1}^*)) = \text{VS}(h((x))) \).

Let \( B^* = \{ x_i^* : i \in P \} \). As \( x^* = \text{Refl}(h((x_0^*))) \) depends on \( x_{j_1,0}, \ldots, x_{j_n,0} \), \( B^*\text{-support}(x^*) \) consists of \( x_i^* \) together perhaps with some \( x_j^* \)'s where \( i < j_n \). Thus, \( x^* = h(x^*) \) depends on \( h((x_{i_1}^*)), \ldots, h((x_{i_m}^*)), h((x_k^*)) \). Thus, \( x^* \) is \( \text{Row} \ j_n \) correct. Thus, as promised we have shown \( x_{j_1,1}, \ldots, x_{j_n,n} \in B_{\text{sq}}\text{-support}(x^*) \).

Proof of (b). \( v \) is \( (y_{0,j}) \) for some \( j \in P \) if and only if there is a \( u \) such that \( u \) is \( (x_{0,j}) \) for some \( j \in P \) and \( v = \text{Id}_{\text{sq}}(u) \). \( \Box \)

Theorem 2.12. Second-order number theory may be reduced to the first-order theory of \( \mathcal{L}^* \).

Proof. By folklore it suffices to show how to interpret quantification over elements of \( P \) and quantification over one-to-one functions from \( P \) into \( P \).

We interpret \( P \) as \( \{ u : P(u) \} \). We interpret the set of one-to-one functions from \( P \) into \( P \) as the set of all codes of a function from \( P \) into \( P \), where a code of a function from \( P \) into \( P \) is a weak code \( F \) of a function from \( \text{Row}0 \) into \( \text{Row}0' \) such that

\[
(\forall i \in P)((x_{0,i}) \in \text{Dom}_F \rightarrow (\exists j \in P)(F((x_{0,i})) = (y_{0,j}))),
\]

that is, \( (\forall u)_{P(u)}(u \in \text{Dom}_F \rightarrow (\exists v)_{P'(u)}(F(u) = v)) \).
We say $F$ codes the function $f$ defined by:

$$f(i) = j \text{ if and only if } F((x_{0,i})) = (y_{0,j}).$$

It remains to observe that any one-to-one function $f$ is coded by some $F$ and hence quantification over codes of functions gives quantification over all one-to-one functions. This is true as if we let $F = (a(x_{0,i}, y_{0,f(i)}: i \in P)$, then $f$ is coded by $F$. \hfill \Box

**Notation.** For any formula $\Phi$ of second-order number theory, we let $\Phi^*(\text{PARAM})$ be the translation (given by the proof of Theorem 2.10) of $\Phi$ into the first-order language of the lattice $\mathcal{L}^*$.

**Theorem 2.13.** Second-order number theory may be reduced to the first-order theory of $\mathcal{L}$.

**Proof.** In order to use the predicate $P(u)$ to interpret the set $P$ and the codes of functions from $P$ into $P$ to interpret one-to-one functions from $P$ into $P$, only a few properties of the parameters are needed. It suffices that $B = \{u: P(u)\}$ is a countably infinite basis of $\text{Row}0$, $B' = \{v: P'(v)\}$ is a countably infinite basis of $\text{Row}0'$, and $\text{Id}_{\text{Row}0}$ maps $B$ one-to-one, onto $B'$.

Thus, if $\Phi$ is a formula of second-order number theory we interpret it as $(\exists \text{PARAM}) \ (\text{Cond(\text{PARAM}) & } \Phi^*(\text{PARAM}))$, where $\text{Cond(\text{PARAM})}$ says

(1) (a) $\{u: P(u)\}$ is a basis of $\text{Row}0$, that is,

$$\neg(\exists X \subseteq \text{Row}0)((\forall u)_{P(u)}(u \subseteq X))$$

& $(\forall u)_{P(u)}(\exists X \subseteq \text{Row}0)((\forall v)_{P'(v)}(v \neq u \rightarrow v \subseteq X)))$, 

(b) $\{v: P'(v)\}$ is a basis of $\text{Row}0'$.

(2) $\text{Id}_{\text{Row}0}$ gives a one-to-one correspondence between $B$ and $B'$, that is,

$$(\forall u)_{P(u)}(\exists! v)_{P'(v)}(\text{Id}_{\text{Row}0}(u) = v) \& (\forall v)_{P'(v)}(\exists! u)_{P(u)}(\text{Id}_{\text{Row}0}(u) = v),$$

(3) $\text{Row}0$ has countably infinite dimension. \hfill \Box

**Conjecture.** If a nontrivial Steinitz Exchange System $S$ has dimension $\kappa > \aleph_0$, then second-order logic on a set of cardinality $\kappa$ may be reduced to the first-order theory of $\mathcal{L}$, the lattice of cl-closed subsets of $S$.

**Remark.** One of the authors, M. Rubin, has proven this conjecture for $\kappa = \aleph_n$, where $1 < n < \omega$. The proof makes further use of ideas from [4] and will appear elsewhere.

**Theorem 2.14.** To prove the above conjecture it suffices to show that with parameters one can define a basis $B$ of some cl-closed set $C$ of dimension $\kappa$.

**Sketch of Proof.** Assume such a basis $B$ has been defined. Write $B$ as a disjoint union of two sets $B_1$ and $B_2$ of cardinality $\kappa$. 
Let \( C_i = \text{cl}(B_i) \). Let \( f \) be a 1–1, onto function from \( B_1 \) to \( B_2 \). Let \( F \) be a weak code of \( f \). Using the additional parameters \( C_1 \) and \( C_2 \) we can define \( B_1 \) and \( B_2 \). Thus, we can interpret quantification over elements of a set (namely \( B_1 \)) of cardinality \( \kappa \).

As \( \kappa > \aleph_0 \), to interpret second-order logic on \( B_1 \) by folklore it suffices also to interpret quantification over all functions from \( B_1 \) into \( B_1 \). This may be done as follows:

**Definition** (in \( \mathcal{L}^* \)). \( H \) is a code of a general function from \( B_1 \) to \( B_2 \) if
\[
(\forall v \in B_1)(\exists! v \in B_2)((u, v) \text{ meet } H \text{ is one dimensional}).
\]

**Definition**. \( H \) encodes the function \( h \) defined by \( h(u) = v \) if and only if \( (u, v) \text{ meet } H \text{ is one dimensional}. \)

**Proposition 2.15.** If \( h \) is a function from \( B_1 \) to \( B_2 \), then \( h \) is encoded by
\[
H = (a(b, h(b)) : b \in B_1).
\]

The crucial point in the proof of this proposition is:

**Lemma 2.16.** If \( b_1, \ldots, b_n \in B_1; a_i = a(b_i, h(b_i)) \) for \( i = 1, \ldots, n \); \( u 1 \subseteq B_1 \); \( v 1 \subseteq B_2 \); \( b = (u \text{ join } v) \text{ meet } H \text{ is one dimensional}; \) and \( b \) depends on \( a_1, \ldots, a_n \); then \( u \) depends on \( b_1, \ldots, b_n \).

The proof of Lemma 2.16 is similar to that of Lemma 2.7.

By Proposition 2.15 we can interpret quantification over all functions from \( B_1 \) to \( B_2 \). Using the parameter \( F \) one can also interpret quantification over all functions from \( B_1 \) to \( B_1 \).

It remains to eliminate the use of parameters. This may be done similarly to Theorem 2.13. Here Cond(\( \text{PARAM} \)) says:

1. \( B_1 \) is a basis of \( C_1 \) and \( B_2 \) is a basis of \( C_2 \),
2. \( F \) gives a one-to-one correspondence between \( B_1 \) and \( B_2 \), and
3. \( B_1 \) has cardinality \( \kappa \).

(3) may be expressed in the first-order theory of \( \mathcal{L}^* \) by
\[
(\exists C_3, K)(C_1 \text{ and } C_3 \text{ are independent } \& \ C_1 \text{ join } C_3 = S \\
\text{ } \& \ K \text{ is a weak code of a function from } C_1 \text{ onto } C_3).
\]

**Section 3**

We use the same notation as in Section 1 except that here \( K \) is an algebraic closed field of characteristic \( p \) and of infinite transcendence degree over its prime field \( k \).

**Theorem 3.1.** The first-order theory of the lattice of algebraically closed subfields of \( K \) has the strength of full second-order logic on the set \( K \).
Proof. For finite characteristic we must modify the proof of Proposition 1.1. to handle inseparable extensions.

Proposition 3.2. \( \text{Id}(x_i, (y_i)) \).

Proof. Left to the reader. □

Proposition 3.3. If \( \text{Id}(u), (v) \), then there is an \( i \in I \) such that \( (u) = (x_i) \) and \( (v) = (y_i) \).

Proof. Assume \( \text{Id}(u), (v) \).

Let \( \{x_i : i \in I_x\} \) be the support of \( u \); \( \{y_i : i \in I_y\} \) be the support of \( v \); \( \{x_i + y_i : i \in I_f\} \) be the support of \( (u \text{ join } v) \) meet \( K_f^\circ \); and \( \{x_i y_i : i \in I_f\} \) be the support of \( (u \text{ join } v) \) meet \( K_g \). By Corollary 2.5, \( I_x = I_y = I_f = I_f^\circ \). Without loss of generality \( I_x = \{x_1, \ldots, x_n\} \). We show \( n = 1 \).

Let \( P_u(U, X_1, \ldots, X_n) \) be an irreducible polynomial of \( u \) over (the rational function field) \( k(x_1, \ldots, x_n) \). Let \( \alpha, \alpha_1, \ldots, \alpha_n \) be maximum such that \( P_u(U, X_1, \ldots, X_n) \) is expressible as \( Q_u(U^{p_1}, X_1^{p_1}, \ldots, X_n^{p_n}) \) (where \( Q_u \) is a polynomial). As we are studying the lattice \( L \) and \( K \) we may replace elements of \( K \) by other elements generating the same one dimensional element of \( L \). In particular we replace \( u \) by \( u^{p_1} \), and for \( i = 1, \ldots, n \) \( x_i \) by \( x_i^{p_1} \), and \( y_i \) by \( y_i^{p_1} \). (As \( (x_i + y_i)^{p_1} = x_i^{p_1} + y_i^{p_1} \), this change of variables does not affect the element \( (x_i + y_i) \) of the lattice. Similarly \( (x_i, y_i) \) is unaffected.) So we may as well assume that \( P_u = Q_u \). It is easy to see that \( P_u \) is an irreducible polynomial of \( u \) over \( k(x_1, \ldots, x_n) \) and that the formal derivatives \( \partial P_u/\partial U, \partial P_u/\partial X_i \) for \( i = 1, \ldots, n \) do not vanish at \( U = u, X_1 = x_1, \ldots, X_n = x_n \).

Let \( P_v(V, Y_1, \ldots, Y_n) \) be an irreducible polynomial of \( v \) over \( k(y_1, \ldots, y_n) \). Let \( \beta, \beta_1, \ldots, \beta_n \) be maximum such that \( P_v(V, Y_1, \ldots, Y_n) \) is expressible as \( Q_v(V^{p_1}, Y_1^{p_1}, \ldots, Y_n^{p_n}) \) (where \( Q_v \) is a polynomial). Replace \( v \) by \( v^{p_1} \). This change of variables leaves \( P_v \) irreducible. Furthermore \( \partial P_v/\partial v \) does not vanish at \( V = v, Y_1 = y_1, \ldots, Y_n = y_n \). By reordering \( 1, \ldots, n \) we may assume \( 0 \leq \beta_1 \leq \beta_2 \leq \ldots \leq \beta_n \). \( P_v(V^{p_1}, Y_1, \ldots, Y_n) \) equals \( Q_v(V^{p_1}, Y_1^{p_1}, \ldots, Y_n^{p_n}) \) and, hence, equals \( [R_v(V, Y_1, \ldots, Y_n)]^{p_1} \) (where \( R_v \) is a polynomial). Replace \( v \) by \( v^{p_1} \). As \( R_v \) is irreducible and \( R_v(v, y_1, \ldots, y_n) = 0 \), we may as well assume that \( P_v = R_v \).

Thus, \( u \) and \( v \) are separable algebraic over \( k(x_1, \ldots, x_n, y_1, \ldots, y_n) \) and the partial derivatives \( \partial u/\partial x_i \) and \( \partial v/\partial y_i \) are well-defined for \( i = 1, \ldots, n \). \( \partial u/\partial x_i = -(\partial P_u/\partial x_i)/(\partial P_u/\partial u) \) at \( U = u, X_1 = x_1, \ldots, X_n = x_n \) and \( \partial v/\partial y_i = - (\partial P_v/\partial y_i)/(\partial P_v/\partial v) \) at \( V = v, Y_1 = y_1, \ldots, Y_n = y_n \). In particular:

(1) \( \partial u/\partial x_i \neq 0 \) for \( i = 1, \ldots, n \) and \( \partial v/\partial x_i \neq 0 \).

As \( u, v, x_1 + y_1, \ldots, x_n + y_n \) are dependent, there is an irreducible polynomial
Some highly undecidable lattices

$S(U, V, Z_1, \ldots, Z_n)$ such that $S(u, v, x_1 + y_1, \ldots, x_n + y_n) = 0$. As $S$ is irreducible one of $\partial S/\partial U, \partial S/\partial V, \partial S/\partial Z_1, \ldots, \partial S/\partial Z_n$ is not identically zero. Hence,

(2) The same one of these partial derivatives is not zero at

$$U = u, \quad V = v, \quad Z_i = x_i + y_i \quad \text{for} \quad i = 1, \ldots, n.$$  

As $0 = S(u, v, x_1 + y_1, \ldots, x_n + y_n)$, differentiation with respect to $x_i$ yields

(3) $(\partial S/\partial U) \cdot (\partial u/\partial x_i) + \partial S/\partial Z_i = 0,$

and differentiation with respect to $y_i$ yields

(4) $(\partial S/\partial V) \cdot (\partial v/\partial y_i) + \partial S/\partial Z_i = 0$

(where these derivatives of $S$ are evaluated at $U = u, \ V = v, \ Z_i = x_i + y_i$ for $i = 1, \ldots, n$).

Using (1), (2), (3), and (4) one may easily deduce that $\partial u/\partial y_i \neq 0$ and

(5) $(\partial u/\partial x_i)/(\partial u/\partial x_1) = (\partial S/\partial Z_i)/(\partial S/\partial Z_1)$

(henceforth, this ratio is denoted as $r_i$) for $i = 1, \ldots, n$.

As in Section 1, $r_i \in \text{cl}(k)$.

As $u, \ v, \ x_1, y_1, \ldots, x_n, y_n$ are dependent, there is an irreducible polynomial $T(U, V, Z_1, \ldots, Z_n)$ such that $T(u, v, x_1, y_1, \ldots, x_n, y_n) = 0$. Reasoning as with $S$ we obtain:

(6) One of $\partial T/\partial U, \partial T/\partial V, \partial T/\partial Z_1, \ldots, \partial T/\partial Z_n$ (evaluated at $U = u, \ V = v, \ Z_i = x_i + y_i$ for $i = 1, \ldots, n$) is not zero;

(7) $(\partial T/\partial U) \cdot (\partial u/\partial x_i) + y_i \cdot (\partial T/\partial Z_i) = 0; \quad \text{and}$

(8) $(\partial T/\partial V) \cdot (\partial v/\partial y_i) + x_i \cdot (\partial T/\partial Z_i) = 0.$

From (1), (5), (6), and (7) one may easily deduce that

(9) $(x_i/x_1) \cdot (\partial u/\partial x_i)/(\partial u/\partial x_1) = (y_i/y_1) \cdot (\partial v/\partial y_i)/(\partial v/\partial y_1)$ for $i = 1, \ldots, n$.

By (5) and (9) $y_i x_i = x_i y_i$ for $i = 1, \ldots, n$. If $n \neq 1$ this contradicts that $x_1, \ldots, x_n, y_1, \ldots, y_n$ are independent. □

Proof of Theorem 3.1 (completed). The proof may be completed either by arguments similar to those in Section 1 or by use of Theorem 2.14. □

References