# Prime ideals yield almost maximal ideals

by

**Andreas Blass** * (Ann Arbor, Mich.)

**Abstract.** We prove that Johnstone's almost maximal ideal theorem follows (in set theory without the axiom of choice) from the Boolean prime ideal theorem. In view of earlier work of Johnstone and of Banaschewski and Harting, this result immediately gives several new equivalents for the Boolean prime ideal theorem, for example the Tychonoff theorem for compact sober spaces and the existence of prime ideals in arbitrary (not necessarily commutative) rings with unit. We also give a combinatorial characterization of the permutation models that satisfy the Boolean prime ideal theorem.

We shall be concerned with three existence principles for ideals in distributive lattices: the maximal ideal theorem, the prime ideal theorem, and the almost maximal ideal theorem. (We adopt the convention that lattices are required to have a bottom element 0 and a top element 1; ideals are subsets that are closed downward and closed under finite joins.)

The maximal ideal theorem asserts that every nontrivial distributive lattice has a maximal (proper, of course) ideal. Klimovsky [10] proved that this theorem is equivalent to the axiom of choice (AC). (The proof will also be in the forthcoming revised edition of [13].) It is well-known that AC is needed for the proofs of many mathematical theorems (see, for example, [7]) and is in fact equivalent to many of them [13]. Among these equivalent theorems are (in addition to the maximal ideal theorem for lattices) the maximal ideal theorem for rings with unit (or just for integral domains) [6] and Tychonoff's theorem that products of compact spaces are compact [9].

Here and throughout this paper "equivalent" means provably equivalent in Zermelo–Fraenkel set theory without the axiom of choice or in the theory obtained from it by deleting the axiom of regularity and weakening the axiom of extensionality to allow the existence of atoms.

The prime ideal theorem, which asserts that every nontrivial distributive lattice has a prime ideal (i.e., an ideal which, whenever it contains the meet of finitely many elements of the lattice, also contains one of those elements), is equivalent [14] to the

* Partially supported by NSF grant MCS 8101560.

special case where the lattice is assumed to be a Boolean algebra. It is therefore usually called the Boolean prime ideal theorem (BPI). It is known [3], [4] to be strictly weaker than AC, but not provable in ZF [2]. Like AC, it is equivalent to many mathematical theorems. Among these are the prime ideal theorem for commutative rings with unit [14], Tychonoff's theorem for compact Hausdorff spaces [11], [7], and the compactness theorem for first-order logic (or just for sentential logic) [5].

Since we shall need to use the fact that BPI implies the sentential compactness theorem, we digress briefly to sketch the proof. Let $\theta$ be a set of sentences built from some sentential variables by means of the usual connectives $\wedge$, $\vee$, and $\neg$. Assume that every finite subset $\theta_0$ is satisfiable by some assignment of truth values to the variables. Sentential compactness asserts that then $\theta$ is also satisfiable. To prove this, define two sentences $\alpha$ and $\beta$ (built from the variables used in $\theta$) to be equivalent if there is a finite $\theta_0 \subseteq \theta$ such that every assignment satisfying $\theta_0$ gives $\alpha$ and $\beta$ the same truth value. Then verify that the equivalence classes form a Boolean algebra, with Boolean operations given by the connectives. The hypothesis of finite satisfiability makes this algebra nontrivial, so BPI provides a prime ideal $I$. Assign to each variable the value *true* (resp. *false*) if its equivalence class is not (resp. is) in $I$, and verify by induction on sentences that this assignment satisfies exactly those sentences whose equivalence classes are not in $I$. Among these are all the sentences in $\theta$, for they are in the equivalence class 1. Thus, the assignment satisfies $\theta$ and the proof sketch is complete.

To introduce the concept of almost maximal ideals, and to simplify some later arguments, it is convenient to define the dual $I^*$ of an ideal $I$ by

$$I^* = \{a \mid \text{for some } i \in I,\ i \vee a = 1\}.$$

Distributivity of the lattice implies that $I^*$ is a filter, i.e., closed upward and closed under finite meets. Note that an ideal $I$ is proper if and only if it is disjoint from $I^*$. To define almost maximal ideals, Johnstone [8] first introduced an operation $j$ on ideals by

$$j(I) = \{a \mid \text{for all } b,\ \text{if } a \vee b = 1 \text{ then } b \in I^*\}.$$

It is easily verified that $j(I)$ is an ideal including $I$ and that $j(I)$ is proper if $I$ is. $j(I)$ is the largest ideal having the same dual as $I$. An ideal $I$ is *almost maximal* if it is prime and $j(I) = I$. Since $j$ preserves properness and maximal ideals are prime, it follows that maximal ideals are almost maximal. Johnstone [8] gives examples showing that almost maximality is strictly intermediate between primeness and maximality.

The almost maximal ideal theorem (AMIT) asserts that every nontrivial distributive lattice has an almost maximal ideal. It is clearly intermediate in strength between AC and BPI. By adapting Halpern's argument [3], Johnstone [8] showed AMIT holds in Mostowski's linearly ordered model [12, 7] and is therefore strictly weaker than AC.

Although it was introduced quite recently, AMIT already has some interesting equivalents (mostly in the topology of locales) and consequences. Johnstone [8] showed that AMIT implies the Tychonoff theorem for compact sober spaces and is equivalent to the assertion that every compact locale has at least one point. Banaschewski and Harting [1] defined Wallman locales (a generalization of compact $T_1$ spaces) and showed that all of these are spatial if and only if AMIT holds. They also deduced from AMIT that every (not necessarily commutative) ring with unit has a prime ideal.



Although Johnstone proved that AMIT is strictly weaker than AC, he left open the question whether it is strictly stronger than BPI. The main result of this paper is a negative answer to this question.

THEOREM 1. *The Boolean prime ideal theorem implies the almost maximal ideal theorem.*

After seeing a preprint of this paper, B. Banaschewski found a considerably shorter proof of this theorem than the one given here. His proof will appear in [0].

Proof. Assume that BPI and therefore the compactness theorem for sentential logic are true. Let $L$ be a nontrivial distributive lattice. We intend to apply compactness to the set $\theta$ of sentences defined as follows.

The sentential variables are to be all the ordered triples $(I, x, y)$ where $I$ is a proper ideal of $L$ and where $x$ and $y$ are elements of $L$ satisfying $x \wedge y \in I$. For each proper ideal $I$, each finite subset $F$ of $L$ whose join $\bigvee F$ is in the dual $I^*$ of $I$, and each function $f\colon F \to L$ such that $x \wedge f(x) \in I$ for all $x \in F$, $\theta$ is to contain the two sentences

$$\xi(I, F, f) := \bigvee_{x \in F} \neg (I, x, f(x)) \quad \text{and}$$

$$\eta(I, F, f) := \bigvee_{y \in F} (I, f(y), y).$$

Note that the restriction on $f$ ensures that the ordered triples occurring in $\xi(I, F, f)$ and $\eta(I, F, f)$ are sentential variables. Note also that no sentence in $\theta$ involves two sentential variables with distinct first components $I$.

To apply (sentential) compactness to $\theta$, we must first verify that every finite $\theta_0 \subseteq \theta$ is satisfiable. Let $\theta_0$ be given; it is the union of finitely many (because $\theta_0$ is finite) subsets $\theta_0(I)$, each consisting of those sentences in $\theta_0$ in which all the variables have first component $I$. We shall show that each $\theta_0(I)$ is satisfied by some assignment of truth values to the variables occurring in it; since these are different variables for different $I$'s, we can simply combine the assignments to satisfy $\theta_0$. (AC is not needed to choose an appropriate assignment for each $I$, since only finitely many $I$'s occur.)

So we concentrate on one of the sets $\theta_0(I)$. Let $Q$ be the set of pairs $(x, y)$ such that $(I, x, y)$ occurs in (at least one formula in) $\theta_0(I)$. By definition of sentential variables, we have $x \wedge y \in I$ for every such pair. Since $I$ is an ideal and $Q$ is finite (because $\theta_0(I)$ is), $I$ contains

$$\bigvee_{(x,y) \in Q} (x \wedge y),$$

which can be rewritten, by distributivity, as

$$\bigwedge_{C}\Big(\big(\bigvee_{(x,y)\in C} x\big)\vee\big(\bigvee_{(x,y)\in Q-C} y\big)\Big),$$

where $C$ ranges over all subsets of $Q$. Since $I$ is proper, this element of $I$ cannot be in the dual filter $I^*$. So there must be a subset $C$ of $Q$ such that

$$\big(\bigvee_{(x,y)\in C} x\big)\vee\big(\bigvee_{(x,y)\in Q-C} y\big)\notin I^*.$$

Fix such a $C$, and assign the value true (resp. false) to $(I, x, y)$ if $(x, y)$ belongs to $C$ (resp. $Q-C$). By choice of $C$, neither the join of

$$\{x|\ \text{for some } y,\ (x, y)\in C\}$$

nor the join of

$$\{y|\ \text{for some } x,\ (x, y)\in Q-C\}$$

(nor even the join of both of these joins) is in $I^*$. Consider any $\xi(I, F, f)$ or $\eta(I, F, f)$ in $\theta_0(I)$. By definition of $\theta$, the join of $F$ is in $I^*$, so $F$ cannot be a subset of either of the two sets just displayed. Thus, $F$ contains an $x_0$ such that $(x_0, y)\notin C$ for any $y$, and $F$ contains a $y_0$ such that $(x, y_0)\notin Q-C$ for any $x$. In particular, $(x_0, f(x_0))\notin C$ and $(f(y_0), y_0)\notin Q-C$. If $\xi(I, F, f)\in\theta_0(I)$, then $(x_0, f(x_0))\in Q$; since $(x_0, f(x_0))\notin C$, the sentential variable $(I, x_0, f(x_0))$ was assigned the value false. This suffices to make $\xi(I, F, f)$ true. If $\eta(I, F, f)\in\theta_0(I)$, then $(f(y_0), y_0)\in Q$; since $(f(y_0), y_0)\notin Q-C$, the sentential variable $(I, f(y_0), y_0)$ was assigned the value true. This suffices to make $\eta(I, F, f)$ true. Thus, the assignment defined above from $C$ makes all sentences in $\theta_0(I)$ true.

As indicated above, such assignments, obtained for (finitely many) different $I$'s, can be combined into an assignment satisfying $\theta_0$. Since $\theta_0$ was an arbitrary finite subset of $\theta$, we can apply the compactness theorem to obtain an assignment $A$ that satisfies $\theta$. Fix such an $A$.

Define, for any proper ideal $I$,

$$X(I) := \{x|\ \text{for some } y,\ A \text{ makes } (I, x, y) \text{ true}\},$$

and consider an arbitrary finite subset $F$ of $X(I)$. For each $x\in F$, let $f(x)$ be such that $A$ makes $(I, x, f(x))$ true; such an $f(x)$ exists as $x\in X(I)$, and the function $f$ can be produced without using AC since $F$ is finite. The choice of $f$ ensures that $A$ makes the sentence $\bigvee_{x\in F}\neg(I, x, f(x))$ false. If the join of $F$ were in the dual filter $I^*$, then this sentence would be an element $\xi(I, F, f)$ of $\theta$, so $A$ would make it true. Therefore, $\bigvee F\notin I^*$. We have shown that no finite subset of $X(I)$ has join in $I^*$, which means that $I\cup X(I)$ generates a proper ideal (consisting of all elements $\leqslant i\vee\bigvee F$ for $i\in I$ and finite $F\subseteq X(I)$) which we call $X^+(I)$.

Similarly, let

$$Y(I) := \{y|\ \text{for some } x,\ A \text{ makes } (I, x, y) \text{ false}\},$$



and consider any finite $F\subseteq Y(I)$. For each $y\in F$, let $f(y)$ be such that $A$ makes $(I, f(y), y)$ false. Thus, $A$ makes $\bigvee_{y\in F}(I, f(y), y)$ false. If $\bigvee F$ were in $I^*$, this sentence would be an element $\eta(I, F, f)$ of $\theta$, so $A$ would make it true. Therefore $\bigvee F\notin I^*$. It follows, as above, that $I\cup Y(I)$ generates a proper ideal $Y^+(I)$.

We define a non-decreasing sequence of proper ideals $I_\alpha$ by the following transfinite recursion.

$$I_0 = \{0\}. \quad \text{(Here we use that } L \text{ is nontrivial.)}$$

$$I_\lambda = \bigcup_{\alpha<\lambda} I_\alpha \quad \text{if } \lambda \text{ is a limit ordinal},$$

$$I_{\alpha+1} = \begin{cases} X^+(I_\alpha) & \text{if } I_\alpha \subsetneqq X^+(I_\alpha),\\ Y^+(I_\alpha) & \text{if } I_\alpha = X^+(I_\alpha) \subsetneqq Y^+(I_\alpha),\\ j(I_\alpha) & \text{otherwise},\end{cases}$$

where $j$ is the operation used in the definition of almost maximality. (Recall that $X^+$, $Y^+$, $j$, and unions of chains all preserve properness of ideals.)

Since there are a proper class of ordinals but only a set of ideals, this transfinite sequence cannot be strictly increasing. So fix an $\alpha$ with $I_\alpha = I_{\alpha+1}$. By definition of $I_{\alpha+1}$, we have

$$I_\alpha = X^+(I_\alpha) = Y^+(I_\alpha) = j(I_\alpha).$$

We shall show that $I_\alpha$ is prime; since $I_\alpha = j(I_\alpha)$, we will then have an almost maximal ideal, as desired.

Suppose $x\wedge y\in I_\alpha$. Then $(I_\alpha, x, y)$ is one of the sentential variables introduced in the definition of $\theta$, so it is assigned a truth value by $A$. If this value is true, then

$$x\in X(I_\alpha)\subseteq X^+(I_\alpha) = I_\alpha.$$

If the value is false, then

$$y\in Y(I_\alpha)\subseteq Y^+(I_\alpha) = I_\alpha.$$

Thus, $x$ or $y$ is in $I_\alpha$, and $I_\alpha$ is prime, as required. ■

By combining Theorem 1 with the results about AMIT in [1] and [8], we obtain several new equivalents of BPI. In the following corollary we list those arising from the equivalents and consequences of AMIT cited earlier. Note that the consequences have become equivalents because they imply BPI.

COROLLARY. *The following are equivalent.*

(a) *The Boolean prime ideal theorem* (BPI).
(b) *The almost maximal ideal theorem* (AMIT).
(c) *Every compact locale has a point.*
(d) *The Tychonoff theorem for compact sober spaces.*
(e) *Every Wallman locale is spatial.*
(f) *Every ring with unit has a prime ideal.* ■

An early version of Theorem 1 established the equivalence between AMIT and BPI only for Fraenkel–Mostowski–Specker permutation models of set theory with atoms; it did this by characterizing the groups and filters of subgroups that give rise to models of AMIT and BPI. Although the equivalence result is, of course, superseded by Theorem 1, the characterization is not and seems to be worth recording. It involves some combinatorial concepts that may be of independent interest. It also shows that the method used by Halpern [3] and Johnstone [8] to prove BPI and AMIT in the ordered Mostowski model, namely to show that an ideal maximal among those with a certain (suitable) invariance group is necessarily prime, is a completely general method; whenever BPI holds in a permutation model, it can be established in this way.

Let $G$ be a group and $X$ a $G$-set, i.e., a set equipped with a left action of $G$. We write the action as multiplication and, if $Y \subseteq X$, we write $gY$ for $\{gy \mid y \in Y\}$. $X$ has the *Ramsey property* if, for every finite $F \subseteq X$, there exists a finite $Y \subseteq X$ such that, whenever $Y$ is partitioned into two pieces, at least one of the pieces includes $gF$ for some $g \in G$.

For example, suppose $X$ is the set $[Q]^n$ of $n$-element sets of rational numbers and $G = \mathrm{Aut}(Q)$ is the group of order-automorphisms of $Q$, with the obvious action on $X$. Since every finite $F \subseteq X$ is included in one of the form $[P]^n$, with $P$ a finite subset of $Q$, the Ramsey property easily reduces to: For every finite $P \subseteq Q$, there exists a finite $Z \subseteq Q$ such that, whenever $[Z]^n$ is partitioned into two pieces, then at least one of the pieces includes $[gP]^n$ for some $g \in G$. Since every subset of $Q$ of the same cardinality as $P$ is $gP$ for some $g \in G$, the Ramsey property for this example amounts to (the finite form of) Ramsey's theorem.

The example relevant to the proofs of BPI and AMIT in the ordered Mostowski model is a generalization of the preceding one. Let $(\mathrm{Aut}(Q))^k$ act componentwise on $[Q]^{n_1} \times \ldots \times [Q]^{n_k}$. The Ramsey property for this example reduces to the assertion that, for any natural numbers $p_1, \ldots, p_k$, there exist finite sets $Z_1, \ldots, Z_k$ such that, whenever $[Z_1]^{n_1} \times \ldots \times [Z_k]^{n_k}$ is partitioned into two parts, then there exist $p_i$-element subsets $H_i \subseteq Z_i$ for $i = 1, \ldots, k$, such that $[H_1]^{n_1} \times \ldots \times [H_k]^{n_k}$ is included in one piece. This assertion is the main combinatorial lemma in [3].

An example of a different sort is given by taking $X = Q$ with $G$ being the group of affine transformations ($x \mapsto ax+b$, with constant $a$ and $b$ in $Q$, and $a \neq 0$). Now every finite $F \subseteq X$ is included in a finite arithmetic progression. It easily follows that the Ramsey property for $X$ amounts to van der Waerden's partition theorem for arithmetic progressions [15].

We leave it to the reader to formulate other well-known partition theorems as instances of the Ramsey property.

A subgroup $H$ of a group $G$ is called a *Ramsey subgroup* if the $G$-set $G/H$ of left cosets $gH$ (with the obvious $G$-action) has the Ramsey property. A normal filter $\mathscr{F}$ of subgroups of a group $\mathscr{G}$ has the *Ramsey property* if it has a basis $\mathscr{B}$ of groups $G$ such that every subgroup of $G$ in $\mathscr{F}$ is a Ramsey subgroup of $G$. (For the definition of normal filters and other concepts related to permutation models, see [7], chapter 4.)



Let $M$ be the permutation model defined by a set $U$ of atoms, a group $\mathscr{G}$ of permutations of $U$, and a normal filter $\mathscr{F}$ of subgroups of $\mathscr{G}$. We may assume that every group $G \in \mathscr{F}$ occurs as the stabilizer of some element of $M$, for if not then the groups that do occur constitute another normal filter that also defines $M$.

THEOREM 2. *With $M$, $U$, $\mathscr{G}$, $\mathscr{F}$ as above, the following are equivalent.*

(a) BPI *holds in $M$.*

(b) *$\mathscr{F}$ has the Ramsey property.*

(c) AMIT *holds in $M$.*

Proof. It is trivial that (c) implies (a). We prove (a)→(b)→(c).

(a)→(b). Assume that $M$ satisfies BPI, and consider an arbitrary $K \in \mathscr{F}$. Define a $K$-set $X$ as follows. Whenever $G, H \in \mathscr{F}$ are subgroups of $K$ and $F$ is a counterexample to the Ramsey property of some $G$-orbit in $K/H$ (i.e., $F$ is a finite subset of a $G$-orbit in $K/H$ and every finite subset $Y$ of that orbit can be partitioned into two pieces neither of which includes $gF$ for any $g \in G$), $X$ will have a subset, called the $(F, G, H)$-orbit, isomorphic as a $K$-set to $K/H$. The orbits labeled by distinct triples $(F, G, H)$ are to be distinct, hence disjoint.

Since every group in $\mathscr{F}$ is the stabilizer of some set in $M$, it is easy to see that $X$ is $K$-isomorphic to some set in $M$, stabilized by $K$, with the $K$-action induced by the action of $\mathscr{G}$ on $M$. For notational simplicity, this set in $M$ will also be called $X$.

Using the members of $X$ as sentential variables, define $\theta$ to consist of the sentences

$$\xi(F, G, H, k) := \bigvee_{x \in F'} \neg kx\,,$$

$$\eta(F, G, H, k) := \bigvee_{x \in F'} kx\,,$$

where $k \in K$, where $(F, G, H)$ labels a $K$-orbit isomorphic to $K/H$ in $X$, and where $F'$ is the image in this orbit, under this isomorphism, of $F \subseteq K/H$. $\theta$ is invariant under $K$ and its members are in $M$, so $\theta \in M$. We intend to apply the sentential compactness theorem to it.

Notice that each sentence in $\theta$ contains sentential variables from only a single $(F, G, H)$-orbit in $X$, and indeed from only a single $K$-translate $kT$ of the $G$-orbit that contains $F'$. Thus, to show that every finite $\theta_0 \subseteq \theta$ is satisfiable, it suffices to treat the case where all sentential variables in $\theta_0$ are in the same set $kT$ of this sort, for then, given an arbitrary finite $\theta_0$, we can treat each of the subsets involving one $kT$ separately and combine the assignments satisfying these subsets into one satisfying $\theta_0$. (An assignment of truth values to finitely many elements of $M$ is, of course, in $M$.) So let a finite $\theta_0 \subseteq \theta$ be given, involving sentential variables from a single $K$-translate $kT$ of the $G$-orbit $T$ containing $F'$ (in the $K$-orbit labeled $(F, G, H)$). Replacing $\theta_0$ by $k^{-1}\theta_0$, we may assume that all variables in $\theta_0$ are in $T$.

Let $Y$ be the set of all the elements of $T$ that occur as variables in $\theta_0$. By the definition of what it means for $(F, G, H)$ to label an orbit in $X$, there must be a partition of $Y$ into two pieces, neither of which includes $gF$ for any $g \in G$. Then all the sentences in $\theta_0$, being of the form $\xi(F, G, H, g)$ or $\eta(F, G, H, g)$ with $g \in G$ (since the variables of $\theta_0$ are from $T$), will be satisfied if we assign the value *true* to all the variables in one piece of this partition of $Y$ and the value *false* to all the variables in the other piece.

Thus, each finite $\theta_0 \subseteq \theta$ is satisfiable. Applying the compactness theorem inside $M$, let $A$ be an assignment of truth values to all the variables in $X$, making all of $\theta$ true. Since $A \in M$, let $G \in \mathscr{F}$ stabilize $A$; replacing $G$ by $G \cap K$, we may assume that $G \subseteq K$.

We shall show that every subgroup $H \in \mathscr{F}$ of $G$ is a Ramsey subgroup. Suppose not, and let $H$ be a counterexample. Let $F$ be a finite subset of $G/H \subseteq K/H$ such that every finite $Y \subseteq G/H$ can be partitioned into two pieces neither of which includes $gF$ for any $g \in G$. Then $(F, G, H)$ labels an orbit in $X$, and $\theta$ contains sentences $\xi(F, G, H, 1)$ and $\eta(F, G, H, 1)$ which require $A$ to assign false to some variables and true to other variables in $F'$. But all the variables in $F'$ lie in the same $G$-orbit in $X$, and $A$ is $G$-invariant, so this is impossible. This contradiction proves that every subgroup of $G$ in $\mathscr{F}$ is a Ramsey subgroup.

We have found a $G \in \mathscr{F}$ with this property inside an arbitrary prescribed $K \in \mathscr{F}$. This means that these $G$'s form a basis for $\mathscr{F}$, so $\mathscr{F}$ has the Ramsey property.

(b)$\to$(c). This is essentially an abstract version of the Halpern–Johnstone argument; indeed, the Ramsey property was found by asking what is needed for that argument to work.

Given a nontrivial distributive lattice $L$ in $M$, choose a $G \in \mathscr{B}$ (the basis given by the Ramsey property of $\mathscr{F}$) stabilizing $L$. By Zorn's lemma in the real world, let $I$ be a maximal $G$-invariant proper ideal of $L$. $G$-invariance implies that $I \in M$. Since $j(I)$ is a proper $G$-invariant (because definable from $L$ and $I$) ideal including $I$, maximality implies that $j(I) = I$. It remains to prove that $I$ is prime.

Suppose $a, b \notin I$ but $a \wedge b \in I$. The ideal generated by $I \cup \{ga \mid g \in G\}$ is $G$-invariant and extends $I$ properly as it contains $a$. So it is the improper ideal, which means that the join of finitely many of the elements $ga$ is in the dual filter $I^*$. Say

$$g_1 a \vee \ldots \vee g_k a \in I^* .$$

Similarly,

$$g_1 b \vee \ldots \vee g_k b \in I^* ;$$

if the sets of $g_i$'s are different in these two formulas, replace them by their union to make them the same.

Let $H$ be the stabilizer in $G$ of the ordered pair $(a, b)$. Then, being a subgroup in $\mathscr{F}$ of $G \in \mathscr{B}$, $H$ is a Ramsey subgroup of $G$. This means that the $G$-orbit $X$ of $(a, b)$, which is isomorphic to $G/H$, has the Ramsey property. Let

$$F = \{g_1(a, b), \ldots, g_k(a, b)\} ,$$



and apply the Ramsey property to obtain $Y = \{y_1(a, b), \ldots, y_n(a, b)\}$, where $y_1, \ldots, y_n \in G$, such that, whenever $Y$ is partitioned into two pieces, one of the pieces includes $gF$ for some $g \in G$.

Since $a \wedge b \in I$ and $I$ is stabilized by $G$ which contains $y_1, \ldots, y_n$, $I$ must contain each $y_i(a \wedge b)$ and therefore also their join

$$\bigvee_{i=1}^{n} y_i(a \wedge b) = \bigvee_{i=1}^{n} (y_i(a) \wedge y_i(b)) = \bigwedge_{C} \Big(\big(\bigvee_{i \in C} y_i(a)\big) \vee \big(\bigvee_{i \notin C} y_i(b)\big)\Big) .$$

Here the first equation follows from the $G$-invariance of $\wedge$ and the second, in which $C$ ranges over all subsets of $\{1, 2, \ldots, n\}$, follows from distributivity.

Consider any term in the last meet in this equation; it is the term

$$\big(\bigvee_{i \in C} y_i(a)\big) \vee \big(\bigvee_{i \notin C} y_i(b)\big)$$

corresponding to a particular $C$. By choice of $Y$, there exists $g \in G$ such that $gF = \{gg_j(a, b) \mid j = 1, \ldots, k\}$ is included in either $\{y_i(a, b) \mid i \in C\}$ or $\{y_i(a, b) \mid i \notin C\}$. In the first case, each $gg_j(a)$, for $j = 1, \ldots, k$, is $y_i(a)$ for some $i \in C$, so the term under consideration is

$$\geqslant \bigvee_{i \in C} y_i(a) \geqslant \bigvee_{j=1}^{k} gg_j(a) = g \bigvee_{j=1}^{k} g_j(a) \in gI^* = I^* ,$$

where we used that $g \in G$ leaves the lattice operations and $I$ and therefore $I^*$ invariant. Similarly, in the second case, the term under consideration is

$$\geqslant \bigvee_{i \notin C} y_i(b) \geqslant \bigvee_{j=1}^{k} gg_j(b) = g \bigvee_{j=1}^{k} g_j(b) \in gI^* = I^* .$$

Thus, the term under consideration is in $I^*$. But it was an arbitrary term in the meet

$$\bigwedge_{C} \Big(\big(\bigvee_{i \notin C} y_i(a)\big) \vee \big(\bigvee_{i \notin C} y_i(b)\big)\Big) ,$$

so this meet is in $I^*$ also, since $I^*$ is a filter. But we saw above that this meet is in $I$, which contradicts the fact that $I$, being proper, is disjoint from $I^*$. ∎

Remark. The only information we used about the operation $j$ is that, for every proper ideal $I$, $j(I)$ is a proper ideal that includes $I$. Thus, BPI implies that, in any non-trivial distributive lattice, each operation with this property fixes at least one prime ideal. In fact, a slight modification of the proof of Theorem 1 shows that any well-ordered set of such operations has a common fixed prime ideal. The modification affects only the last clause in the definition of the sequence $I_\alpha$, which should now read as follows. If $I_\alpha = X^+(I_\alpha) = Y^+(I_\alpha)$, then $I_{\alpha+1} = j(I_\alpha)$ where $j$ is the first operation in the given well-ordered set such that $I_\alpha \subsetneqq j(I_\alpha)$ provided such a $j$ exists, and $I_{\alpha+1} = I_\alpha$ otherwise. Then $I_\alpha = I_{\alpha+1}$ implies that $I_\alpha$ is fixed by all the given operators and, as before, prime.

## References

[0] B. Banaschewski, *Prime elements from prime ideals*, Order 2 (1985), 211–213.
[1] B. Banaschewski and R. Harting, *Lattice aspects of radical ideals and choice principles*, Math. Proc. Cambridge Phil. Soc. Proc. London Math. Soc. (3) 50 (1985), 385–404.
[2] S. Feferman, *Some applications of the notions of forcing and generic sets*, Fund. Math. 56 (1965), 325–345.
[3] J. D. Halpern, *The independence of the axiom of choice from the Boolean prime ideal theorem*, Fund. Math. 55 (1965), 57–66.
[4] J. D. Halpern and A. Lévy, *The Boolean prime ideal theorem does not imply the axiom of choice*, in *Axiomatic Set Theory*, Part I (Proc. Symp. Pure Math. XIII-1) ed. D. Scott, 83–134.
[5] L. Henkin, *Metamathematical theorems equivalent to the prime ideal theorems for Boolean algebras*, Bull. Amer. Math. Soc. 60 (1954) 387–388.
[6] W. Hodges, *Krull implies Zorn*, J. London Math. Soc. (2) 19 (1979), 285–287.
[7] T. Jech, *The Axiom of Choice*, North-Holland 1973.
[8] P. T. Johnstone, *Almost maximal ideals*, Fund. Math. 123 (1984), 197–209.
[9] J. L. Kelley, *The Tychonoff product theorem implies the axiom of choice*, Fund. Math. 37 (1950), 75–76.
[10] G. Klimovsky, *El teorema de Zorn y la existencia de filtros y ideales maximales en los reticulados distributivos*, Rev. Un. Mat. Argentina 18 (1958), 160–164.
[11] J. Łoś and C. Ryll-Nardzewski, *On the application of Tychonoff's theorem in mathematical proofs*, Fund. Math. 38 (1951), 233–237.
[12] A. Mostowski, *Über die Unabhängigkeit des Wohlordnungssatzes vom Ordnungsprinzip*, Fund. Math. 32 (1939), 201–252.
[13] H. Rubin and J. Rubin, *Equivalents of the Axiom of Choice*, North-Holland 1963.
[14] D. Scott, *Prime ideal theorems for rings, lattices, and Boolean algebras*, Bull. Amer. Math. Soc. 60 (1954), 390.
[15] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. 15 (1927), 212–216.

MATHEMATICS DEPARTMENT
THE UNIVERSITY OF MICHIGAN
Ann Arbor, Michigan 48109-1003

*Received 13 May 1985*

# Counting $\Delta_0$ sets

**J. Paris** and **A. Wilkie** (Manchester)

**Abstract.** In this paper we consider the following well-known problem "Let $B$ be a $\Delta_0$-definable set of natural numbers. Is the function $G(n) = |B \cap n|$ also $\Delta_0$-definable?".

We shall show that the answer is *yes* if $B$ is a very sparse set. We shall also show that for any $B$ we can obtain a fair approximation to $G$ which is $\Delta_0$ definable.

**Notation.** The notation we shall use is entirely standard, see for example [1], [2]. In particular we use $\Delta_0^N$ to denote the class of subsets of $N^k$, $k \in N$, definable in the standard model by a $\Delta_0$ formula in the language of first order arithmetic. For a finite set $B$, $|B|$ denotes the number of elements in $B$. All logarithms are to the base 2 and in expressions like $\log(x)$, $x^\alpha$ ($\alpha$ rational), etc. we shall always mean the integer parts of these quantities, whenever they appear in $\Delta_0$ formulae.

**Introduction.** The following problem was previously considered in [1].

"Let $B \in \Delta_0^N$, $B \subseteq N$. Is the function $G$ defined by $G(n) = |B \cap n|$ also in $\Delta_0^N$?"

The general feeling is that the answer to this problem is *no*, for example for $B$ = set of primes. However we shall show in Theorem 5 that the answer is *yes* if $B$ is very sparse. In Corollary 7 we show that in any case we can always obtain a fair approximation to $G$ which is in $\Delta_0^N$.

In what follows let $A \in \Delta_0^N$, $A \subseteq N^{\nu+2}$ and let

$$A_n(\vec{x}) = \{m \mid \langle \vec{x}, m, n\rangle \in A \,\&\, m < n\} \subseteq n .$$

In the lemmas which follow we shall be trying to count $|A_n(\vec{x})|$. To simplify matters we shall omit mention of the parameters $\vec{x}$ although as we shall see it will be critical that our results are uniform in the parameters.

Throughout $n$ will stand for a large natural number. It should be clear that our results are trivial for $n$ small. Throughout this paper we use the notation $f\colon A \Vert\!\!\twoheadrightarrow B$ $f\colon A \Vert\!\!\rightarrow B$, $f\colon A \twoheadrightarrow B$ to denote that $f$ is respectively a bijective, injective, surjective function from $A$ to $B$.

Our first lemma was previously proved in [1] but for the sake of completeness we repeat the proof here.