Some Connections Between Set Theory and Computer Science

Robert Cowen
Department of Mathematics, Queens College, C.U.N.Y.
Flushing, NY 11367

Abstract. Methods originating in theoretical computer science for showing that certain decision problems are NP-complete have also been used to show that certain compactness theorems are equivalent in ZF set theory to the Boolean Prime Ideal Theorem (BPI). Conversely, there is some evidence that set theoretic methods connnected with research on BPI may prove useful in computer science. We survey what is known and then look at some new examples and explore the underlying reasons for the successful application of quite similar methods to solve different problems.

1 Introduction

My first introduction to theoretical computer science came in 1984 when I attended some lectures given by A. S. Fraenkel on NP-complete problems. I was immediately struck by similarities to questions in set theory relating to the Boolean Prime Ideal Theorem. Jan Mycielski has told me that he also made a similar observation in 1975, which he was kind enough to permit me to use in [7]. Probably others have noticed similarities as well. In this talk I will attempt to show how insights from each field can be of use in the other, and to explore the underlying reasons for these connections.

2 NPC and Set Theory

The Prime Ideal Theorem for Boolean algebras (BPI) states that any Boolean algebra has a prime ideal (or equivalently, a maximal ideal). It is weaker than the Axiom of Choice in ZF set theory and can often be used to replace the Axiom of Choice in mathematical arguments. It has many equivalent formulations in ZF set theory (see, for example: [1]-[5], [7], [12]-[15], [18]-[25], [28], [29]). (A very useful general guide to the literature of weak forms of the axiom of choice, including BPI, and what is known about their interdependencies can be found in a database being compiled by Paul Howard [14].) Many equivalents of BPI take the form of compactness principles. These are principles which state, roughly, that an 'object' has a certain property if all finite 'subobjects' have that property. For example, from propositional logic, we have SAT.

- **(SAT)** If every finite subset of a set of propositional clauses is satisiable, the entire set of clauses is satisfiable.

SAT is equivalent to BPI even if the clauses have at most 3 literals each, in which case it is referred to as 3-SAT (see [7]). Another example, from graph theory is P_k.

- (P_k) If every finite subgraph of a graph is k-colorable, the graph is k-colorable.

P_k is equivalent to BPI for each $k \geq 3$ (Läuchli [18]; see also, [7] for a simpler proof of Mycielski, alluded to above). Computer scientists will recognize both these problems, satisfiability of propositional clauses and graph 3-colorability, as belonging to the class of NP-Complete (NPC) decision problems. For another example consider the NPC problem called ONE-IN-THREE SATISFIABILITY by Schaefer [26]: given sets $S_1, ..., S_n$, each having at most three members, is there a set T such that $|T \cap S_i| = 1$, $1 \leq i \leq n$? Let us call such a T an *exact transversal* for the $S_i, 1 \leq i \leq n$; that is, an *exact transversal* for a collection of sets is a set whose intersection with each set in the collection is a singleton. The corresponding compactness theorem, which shall be referred to as **3ET**, is equivalent to BPI (see [7]).

- (**3ET**) Let $\{S_i\}_{i \in I}$ be a collection of sets, where each S_i has at most 3 members. If for every finite $I_0 \subset I$, $\{S_i\}_{i \in I_0}$ has an exact transversal then $\{S_i\}_{i \in I}$ has an exact transversal.

Another interesting NPC problem from Schaefer [26], is: given a finite collection of sets each with at most three members, can the members be colored with two colors so that no set is all one color; we shall refer to such a coloring as a NOT-ALL-EQUAL or N.A.E. COLORING. The following compactness theorem, which we abreviate by **3NAE,** is equivalent to BPI (see [7]).

- (**3NAE**) Let $\{S_i\}_{i \in I}$ be a collection of sets, where each S_i has at most 3 members. If for every finite $I_0 \subset I$, $\{S_i\}_{i \in I_0}$ has an N.A.E. COLORING, then $\{S_i\}_{i \in I}$ has an N.A.E. COLORING.

In all of the above cases, a proof that BPI implies the compactness result is routine; instead of using BPI directly it is usually easier to use an equivalent form, such as a variant of Rado's Selection Lemma (see, for example, Rav [24]). The proof that the compactness result implies BPI, however, is not routine; in all of the above cases a proof can be given which closely parallels the corresponding NPC result (see [7]). We illustrate this parallelism with a new problem. A graph is said to be *(2,1)-colorable* if its vertices can be colored with two colors such that each vertex has at most one neighbor colored with the same color as itself (cf. [6],[10],[32]).

Theorem 1. *The decision problem for (2,1)-colorability is NPC.*

Proof. The problem is surely in NP. We shall show that the NOT-ALL-EQUAL COLORING problem is reducible to graph (2,1)-colorability. Let $\{S_i\}_{i \in I}$ be a finite

indexed collection of sets of cardinality at most three. We can assume each S_i has either two or three elements since no collection containing a singleton can have an N.A.E. COLORING. We shall construct a graph G as follows. For each $S_i = \{x, y, z\}$, G is to contain a triangle as shown in the figure (a). If $S_i = \{x, y\}$, G contains the graph depicted in figure (b). In addition, G will have the graphs shown in the figure (c) which connect selected vertices from the graphs in figures (a) and (b) and serve to insure that, under any (2,1)-coloring, $< i, x >$and $< j, x >$ will get the same color. The transformation defined from a set system $\{S_i\}_{i \in I}$ to graph G is clearly polynomial. It is now trivial to show that G has a (2,1)-coloring if and only if $\{S_i\}_{i \in I}$ has a N.A.E. COLORING.

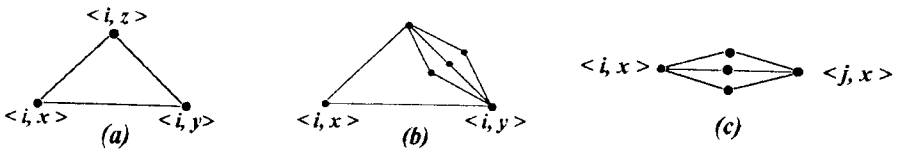

Fig. 1.

The compactness statement for (2,1)-colorings will be denoted by $P_{2,1}$.

- ($P_{2,1}$) If every finite subgraph of a graph is (2,1)-colorable, the graph is (2,1)-colorable.

Theorem 2. *$P_{2,1}$ is equivalent to BPI in ZF.*

Proof. It is routine to show that BPI implies the compactness statement. For the converse, we shall prove 3NAE using $P_{2,1}$.

Let $\{S_i\}_{i \in I}$ be an indexed collection of sets, each of cardinality at most three, such that for every finite $I_0 \subset I$, $\{S_i\}_{i \in I_0}$ has a N.A.E. COLORING. Again, we can assume each S_i has either two or three elements. As in the above NPC proof, we construct a graph G using elements from the figures (a), (b) and (c). Every finite subgraph of G can be (2,1)-colored since for every finite $I_0 \subset I$, $\{S_i\}_{i \in I_0}$ has a N.A.E. COLORING. Therefore, by $P_{2,1}$, G has a (2,1)-coloring; let x have the color assigned to the $< i, x >$. This will be a N.A.E. COLORING of $\{S_i\}_{i \in I}$.

An advantage of having many different formulations of BPI is the same as having many different NPC problems: it facilitates settling new problems as we have just seen in the case of graph (2,1)-colorability.

The above considerations suggest that there may be common principles which underlie both NPC proofs in Computer Science and BPI equivalence proofs of compactness statements in set theory. This is explored in the next section.

3 Logical Embeddings

For any propositional formula ψ, $sat(\psi)$, will denote the set of those interpretations which satisfy ψ. We use "1" and "0" as truth values instead of "t" and "f". The set of propositional variables of ψ will be denoted by $var(\psi)$. Thus, if $V = var(\psi)$, $sat(\psi)$ is a subset of $\{0,1\}^V$. In fact if V is any finite set of variables, any subset of $\{0,1\}^V$equals $sat(\psi)$ for some propositional formula ψ which we can assume is in conjunctive normal form.

- *Definition.* If φ, ψ are propositional formulas, with $var(\varphi) \subset var(\psi)$, $\varphi \prec \psi =_{df} sat(\psi)|_{var(\varphi)} = sat(\varphi)$.

Thus, if $\varphi \prec \psi$, any satisfying assignment of φ can be extended to a satisfying assignment of ψ, and, conversely, any satisfying assisgnment of ψ, when restricted to the variables of φ, will satisfy φ. In particular, φ is satisfiable if and only if ψ is satisfiable.

If φ is a cnf, there exists a cnf ψ, with at most 3 literals per clause, such that $\varphi \prec \psi$; in addition, ψ can be obtained from φ by a polynomial time transformation (see [11], p.48). This is the basis for proving that 3-SAT is NPC, where 3-SAT is the problem of determining whether a cnf with at most 3 literals per clause is satisfiable. I used the same construction to show that the compactness statement for satisfiability of cnfs with at most 3 literals per clause, 3-SAT, is equivalent to BPI (see [7]); here, it is unimportant that ψ is obtainable from φ in polynomial time, only that it can be obtained in a uniform way to avoid arbitrary choices which might necessitate some form of the Axiom of Choice.

If we consider cnfs with only 2 literals per clause, it is no longer true that for any cnf φ, there exits a cnf ψ with only 2 literals per clause, such that $\varphi \prec \psi$. The decision problem for cnfs with 2 literals per clause, 2-SAT, is polynomial ([11]) and the compactness statement, which we shall also refer to as 2-SAT, is weaker than BPI in ZFU, ZF set theory with 'urelements'. (This follows from results in [13] and [19]). Very recently, P. Wojtylak has succeeded in showing that 2-SAT is weaker than BPI in ZF (unpublished).

Let Φ and Ψ be sets of propositional formulas closed under conjunctions and substitutions of propositional variables. Then Φ is *embeddable in* Ψ, $\Phi \prec \Psi$, if for every $\varphi \in \Phi$ there is a $\psi \in \Phi$ such that $\varphi \prec \psi$.

In order to treat the above decision problems and others in a more systematic way, Schaefer [26] introduces *S-formulas*. Let $S = \{R_i^{k_i}\}_{i \in I}$ be a finite set of logical relation symbols, where each $R_i^{k_i}$ stands for a particular subset, $\overline{R}_i^{k_i} \subseteq \{0,1\}^{k_i}$. Then an *S-formula* is a finite conjunction of 'clauses', $R_i^{k_i}(\xi_1, ..., \xi_{k_i})$, where the $(\xi_1, ..., \xi_{k_i})$ is a sequence of, not necessarily distinct, propositional variables; let Ψ_S stand for the set of *S-formulas*. An *interpretation* of an *S-formula* is an assignment of 0 or 1 to each of its variables ξ_i; the interpretation

is said to *satisfy* the *S-formula* if and only if $(\overline{\xi}_1, ..., \overline{\xi}_{k_i}) \in \overline{R}_i^{k_i}$, for each of its clauses, $R_i^{k_i}(\xi_1, ..., \xi_{k_i})$, where $\overline{\xi}_i$ is the truth value assigned to ξ_i. For a given S, the problem of deciding *S-formula* satisfiability is referred to as SAT(S). Schaefer [26] proved the following result.

Theorem 3. *SAT(S) is polynomial time decidable if at least one of the following conditions, (a)-(f), holds; otherwise SAT(S) is NP-Complete. (a) (1,...,1)$\in \overline{R}$, for every R in S. (b) (0,...,0)$\in \overline{R}$,for every R in S. (c) Every relation of S is definable by a cnf in which each conjunct has at most 1 negated variable. (d) Every relation of S is definable by a cnf in which each conjunct has at most 1 unnegated variable. (e) Every relation of S is definable by a cnf in which each conjunct has at most 2 literals. (f) Every relation of S is the solution set of a system of linear equations over the 2 element field $GF(2)$.*

The proof turns on whether or not whether Ω, the set of all propositional formulas can be embedded in the set Ψ_S of *S-formulas;* only if **none** of (a)-(f) holds is this the case. Since the cases (a)-(f) are 'logically impovrished', it is hard to see how the compactness statement for Ψ_S in these cases could be used to prove, say, the compactness of propositional logic. This led me to conjecture that all of the following compactness theorems are weaker than BPI.

- If every finite subset of a set of clauses, each containing at most 1 negated variable, is satisfiable, then the entire set is satisfiable.
- If every finite subset of a set of clauses, each containing at most 1 unnegated variable, is satisfiable, then the entire set is satisfiable.
- If every finite subset of a set of clauses, each containing at most 2 literals, is satisfiable, then the entire set is satisfiable.
- If every finite subset of a set of linear equations over the 2 element field $GF(2)$ is satisfiable, then the entire set is satisfiable over $GF(2)$.

The first two conjectures were proved correct by Howard and Höft (unpublished); in fact both are provable in ZF. The third conjecture is 2-SAT, discussed above. The last conjecture is still not settled; it has the following rather odd formulation, due to S. Hechler and myself. A set, Σ, will be said to meet $\{S_i\}_{i\in I}$ *evenly* (*oddly*) if $\Sigma \cap S_i$ consists of an even (odd) number of elements. (Note that we allow $\Sigma \cap S_i = \emptyset$ in the even case.)

- Let $\{S_i\}_{i\in I}$, $\{S_j\}_{j\in J}$ be indexed collections of finite sets with $I \cap J = \emptyset$. Then there is a set Σ which meets $\{S_i\}_{i\in I}$ evenly and $\{S_j\}_{j\in J}$ oddly, if, for each finite $I' \subset I$, and finite $J' \subset J$, there is a set Σ' which meets $\{S_i\}_{i\in I'}$ evenly and $\{S_j\}_{j\in J'}$ oddly.

If $\Omega \prec \Psi_S$, and the embedding can be specified so that arbitrary choices are unnecessary, then the compactness statement for Ψ_S will be equivalent to BPI. It is interesting to note that a similar embedding result, called the COLORING EXTENSION LEMMA, is at the heart of Läuchli's proof in [18] that $P_3 \Rightarrow$BPI;

Läuchli shows that an arbitrary set of binary partitions of a set E (equivalent to a subset of $\{0,1\}^E$!) equals the set of partitions induced on E by 3-colorings of some graph G whose vertex set includes the set E. It seems that this embedding of Ω, or some equivalent, is at the bottom of every proof that a compactness result is equivalent to BPI. Can the same be said for proofs of NP-Completeness? Schaefer [27], section 3, suggests that this is, indeed, the case.

4 A Conjecture Relating BPI and NPC

In order to further explore connections between BPI and NPC in a more general setting than propositonal logic we adopt the following notation of [7]. Let R be a compactness statement for a set S of mathematical 'objects' and a property P; that is, R asserts that if every finite 'subobject' of an object in S has P, then the object has P. In addition, we shall assume that R is not provably equivalent in ZF to the assertion: every object in S has property P. This last conditon, which did not appear in [7], serves to eliminate certain bogus compactness statements such as: if every finite subalgebra of a boolean algebra has a prime ideal, then the algebra has a prime ideal. This is equivalent to BPI, since it is provable in ZF that finite boolean algebras have prime ideals. Also eliminated is: if every finite subgraph of a graph in Γ is 3-colorable then the graph is 3-colorable, where Γ is the set of graphs whose finite subgraphs are 3-colorable.

If R is a compactness statement, R^* will denote the corresponding finite decision problem which asks for a finite object in the class, does it have property P. $R <$BPI, shall mean that R is weaker than BPI in ZF (without the Axiom of Choice).

It might be thought, from a consideration of the examples above, that if $P \neq NP$, then $R <$BPI $\Leftrightarrow$ R^* is polynomial. However, Kolany and Wojtylak [17] have shown that if R is taken to be SAT with the added restriction that each propositional variable occurs in only finitely many clauses, then $R <$ BPI; surely R^* is NPC, since it is equivalent to the decision problem SAT. A similar example, due to Mycielski, takes R to be P_n, restricted to locally finite graphs (a graph is *locally finite* if all its vertices hav finite degrees). Again, $R <$ BPI, while R^* is NPC. In the opposite direction, I don't know of any counter examples and have made the following conjecture in [7].

- *Conjecture.* If R^* is polynomial, then $R <$ BPI.

This implies, in particular, that $P \neq NP$; since, letting R=P_3, gives $R \Leftrightarrow$ BPI; yet R^* would be polynomial if $P = NP$. The conjecture made above about the compactness of linear equations over $GF(2)$ also follows from this conjecture, since R^* is polynomial, because linear equations are solvable by Gaussian Elimination. If R is the compactness statement that a collection of finite sets has a system of distinct representatives (SDR) if every finite subcollection has an SDR, then again R^* is polynomial and I have conjectured in [7] that $R <$ BPI.

5 BPI and Computer Science

We have seen how very clever constructions used in NPC proofs can be adapted to prove certain compactness statements equivalent to BPI. No doubt more examples will be found. To show, conversely, that set theory, and in particular research involving BPI can have application to computer science we consider yet another compactness principle, the DISJOINT TRANSVERSALS AXIOM OR DTA, due to Schrijver [28]. Let $\mathcal{U}$ and $\mathcal{V}$ be sets of subsets of a set X. A subset Y of X is called a *$\mathcal{U}$-transversal* if $U \cap Y \neq \emptyset$ for all $U \in \mathcal{U}$. Let $\mathrm{dt}(\mathcal{U}, \mathcal{V})$ denote the statement that there exists a $\mathcal{U}$-transversal and a $\mathcal{V}$-transversal which are mutually disjoint.

- (DTA). If X is a set, $\mathcal{U}$, $\mathcal{V}$ collections of finite subsets of X such that $\mathrm{dt}(\mathcal{U}', \mathcal{V}')$, for any two finite subcollections $\mathcal{U}' \subset \mathcal{U}$, $\mathcal{V}' \subset \mathcal{V}$, then $\mathrm{dt}(\mathcal{U}, \mathcal{V})$.

The following theorem is then due to Schrijver[28].

Theorem 4. *DTA is equivalent to BPI in ZF.*

A subset Y of X is termed *$\mathcal{U}$-independent* if no $U \in \mathcal{U}$ is contained in Y. Then, as Schrijver remarks, $\mathrm{dt}(\mathcal{U}, \mathcal{V})$ iff there exists a $\mathcal{U}$ -independent $\mathcal{V}$-transversal. But this implies the following duality principle, since $\mathrm{dt}(\mathcal{U}, \mathcal{V}) \Leftrightarrow \mathrm{dt}(\mathcal{V}, \mathcal{U})$.

- There exists a $\mathcal{U}$-independent $\mathcal{V}$-transversal if and only if there exists a $\mathcal{V}$-independent $\mathcal{U}$-transversal.

Recently Kolany and I have been investigating a general setting for satisfiability problems of various types including satisfiability of propositional clauses, graph colorability, etc. The setting we chose is satisfiability in a hypergraph (see [8],[9],[16]). Methods of proving hypergraph satisfiability, such as a generalized resolution technique and a tableau method, are also considered. It turns out that the definition of hypergraph satisfiability given in Kolany [16] is essentially the same as Schrijver's definition of a $\mathcal{V}$-independent $\mathcal{U}$-transversal. Moreover Schrijver's Duality Principle gives immediately dual proof procedures which were not obvious to us and may in certain cases lead to shorter proofs (see [9]).

Schrijver was concerned with infinite set theoretic questions relating to BPI and formulated compactness statements which, for the most part, turn out to be equivalent to BPI. However the structures and definitions he considered will also, I believe, turn out to be very useful for finite discrete math and computer science. We note also that the existence of a $\mathcal{U}$-independent $\mathcal{U}$-transversal is usually referred to as $\mathcal{U}$ having property **B** (**"B"** stands for the mathematician, F. Bernstein) and has been found useful in finite graph theory(see for example, Woodall [31]). We state one last compactness result and then strenghten Schrijver's Theorem.

- **(B)** A collection $\mathcal{U}$ of finite sets has property B if every finite subcollection has property B.

Theorem 5. **B** *is equivalent to BPI in ZF, even if all sets in* $\mathcal{U}$ *have cardinality at most 3.*

Proof. A little reflection reveals that **B,** with the added restriction on $\mathcal{U}$, is the same as **3NAE**!

The moral is, I suppose, that researchers in both set theory and computer science are studying similar objects: graphs, conjunctive normal forms, set systems,etc. and their interrelations; advances in one area can then often be of use in the other. As always, it pays to be aware of what the other fellow is doing!

References

1. A. Abian: Generalized completeness theorem and solvability of systems of boolean polynomial equations, Zeitschrift für Mathematische Logik, 16(1970), 263-264.
2. B. Banaschewski: The power of the ultra-filter theorem, Journal of the London Mathematical Society, ser. *2,* 27(1983), 193-202.
3. R. Cowen: Some combinatorial theorems equivalent to the prime ideal theorem, Proceedings of the American Mathematical Society, 41(1973), 268-273.
4. R. Cowen: Partition principles for properties of finite character, Reports on Mathematical Logic, 14(1982), 23-28.
5. R. Cowen: Compactness via prime semilattices, Notre Dame Journal of Formal Logic, 24(1983), 199-204.
6. L. Cowen, R. Cowen, D. Woodall: Defective colorings of graphs in surfaces: partitions into subgraphs of bounded valency, J. Graph Theory, 10(1986), 187-195.
7. R. Cowen: Two hypergraph theorems equivalent to BPI, Notre Dame Journal of Formal Logic, 31(1990), 232-239.
8. R. Cowen: Hypergraph Satisfiability, Reports on Mathematical Logic, 24(1991), 113-118.
9. R. Cowen: Combinatorial Analytic Tableaux, to appear.
10. M. Frick: A survey of (m,k)-colorings. In J. Gimbel, J.W. Kennedy, L.V. Quintas (eds.): Quo Vadis, Graph Theory? (Annals of Discrete Math 55), North Holland, 1993.
11. M. Garey, D. Johnson: Computers and Intractability, W. H. Freeman, San Francisco, 1979.
12. L. Henkin: Boolean representation through propositional calculus, Fundamenta Mathematica, 41(1954), 89-96.
13. P. Howard: Binary consistent choice on pairs and a generalization of König's infinity lemma, Fundamenta Mathematica, 121(1983), 31-37.
14. P. Howard: Weak forms of the Axiom of Choice, unpublished.
15. T. Jech: The Axiom of Choice, North Holland, Amsterdam, 1973.
16. A. Kolany: Satisfiability on hypergraphs, Studia Logica, to appear.
17. A. Kolany, P. Wojtylak: Restricted versions of the compactness theorem, Reports on Mathematical Logic, 25(1991), 91-103.
18. H. Läuchli: Coloring infinite graphs and the Boolean prime ideal theorem, Israel Journal of Mathematics, 9(1971), 422-429.
19. A. Levy: Remarks on a paper by J. Mycielski, Acta Mathematica Academiae Sceintiarum Hungaricae, 14(1963), 125-130.
20. J. Łoś, C. Ryll-Nardzewski: On the application of Tychonoff's theorem in mathematical proofs, Fundamenta Mathematica, 38(1951), 233-237.

21. J. Łoś, C. Ryll-Nardzewski: Effectiveness of the representation theory for Boolean algebras, Fundamenta Mathematica, 41(1955), 49-56.
22. J. Mycielski: Some remarks and problems on the coloring of infinite graphs and the theorem of Kuratowski, Acta Mathematica Academiae Scientiarum Hungaricae, 14(1963), 125-130. Errata, ibid., 18(1967), 339-340.
23. J. Mycielski: Two remarks on Tychonoff's product theorem, Bulletin Academie Polonaise des Sciences, 12(1964), 439-441.
24. Y. Rav: Variants of Rado's Selection Lemma and their applications, Mathematische Nachrichten, 79(1977), 145-165.
25. H. Rubin, D. Scott: Some topological theorems equivalent to the Boolean prime ideal theorem, Bulletin of the American Mathematical Society, 60(1954), 389.
26. T. Schaefer: The complexity of satisfiability problems, Proceedings of the 10th Annual ACM Symposium on the Theory of Computing, 216-226, 1978.
27. T. Schaefer: Complexity of decision problems based on finite two-person perfect-information games, Proceedings of the 8th Annual ACM Symposium on the Theory of Computing, 41-49. 1976.
28. A. Schrijver: The dependence of some logical axioms on disjoint transversals and linked systems, Colloquium Mathematicum, 39(1978), 191-199.
29. D. Scott: Prime ideal theorems for rings, lattices and Boolean algebras, Bulletin of the American Mathematical Society, 60(1954), p. 390.
30. L. Stockmeyer: Planar 3-colorability is polynomial complete, SIGACT News 5, 3(July 1973), 19-25.
31. D. Woodall: Property B and the four-colour problem. In: D.J.A. Welsh, D.R. Woodall(eds.): Combinatorics, IMA, 1972.
32. D. Woodall: Improper colourings of graphs. In: R. Nelson, R.J. Wilson(eds.): Graph Colourings, Pitman Research Notes in Mathematics Series, Longman Scientific and Technical, 1990.