Acta Informatica 22, 253-275 (1985)

Acta Informatica

Short Proofs for Tricky Formulas

Balakrishnan Krishnamurthy

Tektronix, Inc.*, M.S. 50-662, P.O. Box 500, Beaverton, OR 97077, USA

Summary. The object of this paper is to demonstrate how certain tricky mathematical arguments can be encoded as short formal proofs for the propositional tautologies representing the mathematical statements. Using resolution as a base proof system for the propositional calculus, we exhibit these short proofs under resolution augmented by one of two principles: the *principle of extension*, originally suggested by Tseitin, and the *principle of symmetry*, introduced in this paper. These short proofs illustrate the power of extension and symmetry in theorem proving.

The principle of extension allows the introduction of auxiliary variables to represent intermediate formulas so that the length of a proof can be significantly reduced by manipulating these variables instead of the formulas that they stand for. Symmetry, on the other hand, allows one to recognize that a tautology remains invariant under certain permutations of variable names, and use that information to avoid repeated independent derivations of intermediate formulas that are merely permutational variants of one another.

First we show that a number of inductive arguments can be encoded as short formal proofs using either extension or symmetry. We provide the details for the tautologies derived by encoding the statement, "An acyclic digraph on n vertices must have a source." We then consider the familiar checkerboard puzzle which asserts that a checkerboard, two of whose diagonally opposite corner squares are removed, cannot be perfectly covered with dominoes. We demonstrate short proofs for the tautologies derived from the above assertion, using extension to mimic the tricky informal argument. Finally, we consider statements asserting the Ramsey property of numbers much larger than the critical Ramsey numbers. We show that the proof of Ramsey's theorem can be imitated using the *principle of symmetry* to yield short proofs for these tautologies.

The main theme of the paper is that both extension and symmetry are very powerful augmentations to resolution. We leave open whether either extension or symmetry can polynomially simulate the other.

* This work was performed while the author was with the General Electric Research Center

1. Introduction

It is well-known that for every propositional formula F there exists a formula F' in conjunctive normal form (CNF) such that the length of F' is at most a polynomial in the length of F and F' is satisfiable iff F is satisfiable. On the other hand, there are short formulas for which any equivalent formula in CNF is necessarily long (see [1]). More precisely, for every polynomial $p(n)$, there is a formula F such that any equivalent formula in CNF is of length at least $p(|F|)$, where $|F|$ represents the length of F. Here "equivalent" means that the two formulas yield the same value for all truth assignments. So, F is equivalent to G iff $(F \equiv G)$ is a tautology.

The above two observations display the fact that preserving satisfiability is much weaker than requiring equivalence. More strikingly, whereas every formula can be transformed to a formula in 3-CNF (see definition below) preserving satisfiability (see [5]), such a transformation is often not possible if we wish to preserve equivalence. For example, for $n \geqq 4$, the formula $(X_1 \equiv X_2 \ldots \equiv X_n)$ has *no* equivalent 3-CNF representation – however long.

All of these efficient transformations map a formula on n variables to a formula on more than n variables. The additional variables are used to represent common sub-expressions in the formula. (In combinational networks, these additional variables often correspond to fan-out nodes.) Thus the introduction of additional variables can be used to advantage in the efficient encoding of Boolean functions.

One of the first to report this observation was Tseitin [16], where he demonstrates propositional formulas that require exponentially long proofs under certain proof systems. He then observes that if one were allowed to introduce auxiliary variables to stand for intermediate formulas, then by manipulating these new variables instead of the formulas that they stand for, one can reduce a proof of exponential length into one of polynomial length. He called the introduction of new variables the *principle of extension.*

Tseitin has suggested that it is possible to encode certain concise mathematical arguments as short formal proofs with the use of the principle of extension. In this paper we illustrate short proofs for some interesting formulas in the propositional calculus by encoding the tricky mathematical arguments used to establish the validity of the formulas. To this end we suggest an augmentation to proof systems – similar in vein to Tseitin's extension called the *principle of symmetry.*

The motivation for this principle comes from the fact that in the course of a mathematical proof, one often uses an arbitrary element of a set as a representative of the set, provided the set possesses sufficient symmetry so that the ensuing arguments equally apply to all other elements of the set. In a similar spirit, the principle of symmetry allows one to recognize that a tautology remains invariant under certain permutations of variable names and uses that information to avoid repeated independent derivations of intermediate formulas that are merely permutational variants of one another.

We show how these two principles can be used to encode short mathematical proofs for certain formulas in the propositional calculus. In the next section

we formally define the notions of extension and symmetry and derive some preliminary results about them. In Sect. 3 we present formulas that yield short proofs using either of the two principles. In Sects. 4 and 5 we demonstrate the power of extension and symmetry, respectively. We conclude in Sect. 6 with a few open problems.

2. Definitions and Notations

We shall assume that the reader is familiar with the propositional calculus. For a formal description of the calculus, see e.g. [12]. Propositional variables will be called *variables*, and well-formed formulas will be called *formulas*. Variables will be distinguished from *literals*, which are variables with an assigned parity of 1 or 0, (also called *positive* and *negative*, respectively). Formulas therefore contain literals, not variables. (Nonetheless, this distinction will be ignored whenever it is convenient but not confusing.) The *complement* of a literal is the literal with the opposite parity. A formula contains literals and connectives $-\bigwedge$, $\bigvee$, $\rightarrow$, $\equiv \sim$, etc. (Even though parentheses will be used to represent formulas, it is well-known that they are not necessary and only serve as a convenience.)

A *truth assignment* to a formula F is a map from the set of variables in F to the set {TRUE, FALSE}. The *value of F under the truth assignment* (or equivalently, the result of the truth assignment on F) will be defined in the usual sense. A formula will be said to be *satisfiable* if for some truth assignment the value of the formula is TRUE. Otherwise, it will be called *unsatisfiable*. A formula is a *tautology* if its value is TRUE for every truth assignment. Observe that a formula F is unsatisfiable iff $\sim F$ is a tautology. A formula is said to be in *conjunctive normal form* (CNF) if the formula is a conjunct of disjuncts of literals (see [4]). It is said to be in *disjunctive normal form* (DNF) if it is a disjunct of conjuncts of literals. In either case, the disjuncts in CNF and the conjuncts in DNF are called *clauses*. A formula is in 3-CNF (3-DNF) if it is in CNF (DNF) with at most three literals in each clause. When F is in CNF (or in 3-CNF), we will often consider F as a set of clauses, as opposed to a formula. A clause will then be a member of F. In the same spirit, we will talk of a literal (and sometimes by abuse of terminilogy, even a variable) being a member of a clause. It will be understood that two literals of the same variable, but with opposite parities, will not be in the same clause. We will distinguish a special clause called the *empty clause*, containing no literals. We will denote the empty clause by $\square$. If F is a formula in CNF, $|F|$ will denote the number of clauses.

We shall define a *proof system* to be one that proves the unsatisfiability of a formula. Informally, a proof system provides a set of *inference rules* that allow the derivation of a formula from a set of formulas. A *derivation or proof* of F from a set of formulas Γ is a sequence $F_1, F_2, \ldots, F_n$ where

i) each F_i is either a formula in Γ or derived from the previous F_i's using a derivation rule in the proof system, and

ii) $F_n = F$.

We denote the statement that there is a proof of F from Γ under the proof system Δ, by $\Gamma \vdash_{\Delta} F$. (We sometimes omit Δ from this notation for brevity.) F is said to be a *logical consequence* of Γ if every truth assignment satisfying all the formulas in Γ also satisfies F. We represent this by $\Gamma \models F$. Observe that the definition of logical consequence is independent of the proof system. If a proof system Δ has the property that $\Gamma \vdash_{\Delta} F$ whenever $\Gamma \models F$ we say Δ is *complete*. Δ is said to be *sound* if $\Gamma \models F$ whenever $\Gamma \vdash_{\Delta} F$.

We will be specifically concerned with the resolution procedure (R) (see [15]) restricted to the propositional calculus. Resolution operates on a CNF representation of a propositional formula and produces new clauses by resolving old clauses. The proof can be represented as a tree – often referred to as a *proof tree*. (A thorough account of the resolution procedure can be found in [4].) Even though a proof will be viewed as a tree, the *complexity* or the *length of a proof* will be measured by the number of distinct clauses in the proof – not by the number of nodes in the tree. In othr words, if the clauses at different nodes of a proof tree are the same, then that clause will be counted only once. This is consistent with the traditional concepts of the length of a proof such as in [10].

In an attempt to demonstrate propositional formulas that require exponentially long resolution proofs, Tseitin [16] suggested a class of formulas. In the same paper he demonstrated that those very formulas admitted short proofs if resolution were augmented by a principle that he called extension. It has been observed that the principle of extension is applicable to a variety of proof systems and it has been shown [8, 14] that whenever two reasonable proof systems (such as resolution) are augmented with extension, the two resulting proof systems are polynomially transformable (i.e., their worst-case complexities differ at most by a polynomial). Hence, it is sufficiently general to study the power of extension in the setting of a specific proof system. In this paper we will restrict ourselves to resolution as a base proof system and define extension and symmetry as augmentations for resolution. However, these principles can be equally applied to any Frege system, as defined by Cook and Reckhow in [8]. Recall that resolution is a proof system for unsatisfiable formulas and the contradiction to be proved is represented as a set of clauses. The *rule of extension* allows the definition of new variables by adding new clauses representing the formula – $X \equiv f(\cdot)$, where X is the new variable and f is a Boolean function of existing variables (including the new ones previously defined). The soundness of extended resolution (ER) has been shown in [6].

Let C be a clause and σ a permutation of the set of variables occurring in C. Define $\sigma(C)$ in the natural way (i.e., the clause obtained by applying σ to each variable in C). Observe that C should really be viewed as a set of literals, but we will omit that level of detail. For a set of clauses S, define $\sigma(S)$ as $\{\sigma(C) | C \in S\}$. Let Σ_S be the group of permutations of the variables in S that leave S invariant, i.e., for all σ in Σ_S $\sigma(S) = S$. The rule of symmetry allows the following derivation:

$$\frac{F; \sigma \in \Sigma_S}{\sigma(F)}.$$

We define symmetric resolution I (SR-I) as resolution augmented with the rule of symmetry.

Our first theorem asserts that SR-I is sound. We prove this by transforming an SR-I proof into a resolution proof and then appealing to the soundness of resolution (see [4]).

Lemma 2.1. *If* $S \vdash_{\text{SR-I}} C$, *then* $S \vdash_R C$.

Proof. By induction on the number of applications of the rule of symmetry. In the basis step, if there are no applications of the symmetry rule, the SR-I proof, say π, is itself a resolution proof. Inductively, we will eliminate one application of the symmetry rule. Suppose A' is derived in π using A and $\sigma \in \Sigma_S$. Further assume that it is the first application if the symmetry rule. Thus the derivation π_A of A in π is, in fact, a resolution proof. We can then transform π_A into π'_A by a uniform application of σ throughout π_A. Clearly this is a resolution proof for A'. Thus we have thus transformed π into π' with one fewer application of the symmetry rule. The lemma follows by induction.

We can now conclude:

Theorem 2.2. *If* $S \vdash_{\text{SR-I}} C$, *then* $S \models C$.

Observe that in the proof of Lemma 2.1 all that is required of σ is that $\sigma(\pi_A)$ remain a valid proof. That is, for every axiom $B \in S$ used in the proof π_A, the permuted formula $\sigma(B)$ must also be an axiom (i.e., $\sigma(B) \in S$). Thus we can permit the inference of A' from a derivation for A as long as there is a permutation σ such that the set of clauses obtained by applying σ to the axioms used in the derivation of A are all axioms in S. This will yield a more powerful rule of symmetry. The corresponding symmetric resolution proof system will be called SR-II. The soundness of SR-II can likewise be proved. In the sequel we will use SR to mean SR-I.

3. Inductive Arguments

Cook [7] showed that there are short ER proofs for tautologies derived from the pigeonhole principle. We show that there are short ER, as well as SR, proofs imitating a number of simple inductive arguments. The interest in these proofs stems from the observation that without extension or symmetry these proofs *seem* to be necessarily of exponential length.

In this paper we provide one example showing how an inductive argument is imitated. This example is drawn from the fact that every acyclic finite digraph must have a source. However, we cannot encode this statement as is since encoding acyclicity seems to require exponential length. To avoid this we encode the negation of the following fact.

Fact 3.1. Every finite transitive digraph with no two cycles must have a source.

Let $n \geqq 3$ be the number of vertices in the digraph. For $1 \leqq i, j \leqq n$, $i \neq j$, let the propositional variable $X_{i,j}$ stand for the statement: "There is a directed

edge from node i to node j." We encode an unsatisfiable formula F_n as:

$$F_n = [\bigwedge_{\substack{1 \leqq i,j,k \leqq n \\ i \neq j \neq k \neq i}} (X_{i,j} \wedge X_{j,k}) \Rightarrow X_{i,k}] \wedge [\bigwedge_{\substack{1 \leqq i,j \leqq n \\ i \neq j}} (\bar{X}_{i,j} \vee \bar{X}_{j,i})]$$
$$\wedge [\bigwedge_{1 \leqq j \leqq n} (\bigvee_{\substack{1 \leqq i \leqq n \\ i \neq j}} X_{i,j})]. \tag{3.1}$$

The first part of the conjunct indicates that the digraph is transitive, the second part indicates that there are no 2-cycles, and the third part asserts that there is no source node. The inductive proof proceeds by identifying two of the n vertices and reducing the problem to a similar digraph on $n-1$ vertices. This is imitated by defining new variables $Y_{i,j}$, $1 \leqq i, j \leqq n-1$ and $i \neq j$, by adding the following sets of clauses:

$$Y_{i,j} \equiv X_{i,j} \quad \text{for } 1 \leqq i,j \leqq n-2,\ i \neq j, \tag{3.2}$$

$$Y_{i,n-1} \equiv X_{i,n-1} \wedge X_{i,n} \quad \text{for } 1 \leqq i < n-1, \tag{3.3}$$

$$Y_{n-1,i} \equiv X_{n-1,i} \vee X_{n,i} \quad \text{for } 1 \leqq i < n-1. \tag{3.4}$$

These definitions are stated as clauses in CNF and these clauses, together with the clauses in F_n, are combined using the resolution rule to derive F_{n-1} stated over the Y variables. Observe that clauses involving $Y_{i,j}$, $i, j \leqq n-2$, remain unchanged. We will show how a typical set of clauses corresponding to the formula

$$Y_{i,j} \wedge Y_{j,n-1} \Rightarrow Y_{i,n-1} \tag{3.5}$$

can be derived. Instead of providing the gory details of a resolition derivation, we will present the derivation informally and leave it to the reader to transform this into a resolution proof.

We will use the following two axioms from Eq. (3-1):

$$X_{i,j} \wedge X_{j.n-1} \Rightarrow X_{i,n-1}, \tag{3.6}$$

$$X_{i,j} \wedge X_{j,n} \Rightarrow X_{i,n} \tag{3.7}$$

and the indicated implications from the defining Eqs. (3.3) and (3.4):

$$Y_{j,n-1} \Rightarrow X_{j,n-1} \wedge X_{j,n}, \tag{3.8}$$

$$Y_{i,n-1} \wedge X_{i,n} \Rightarrow Y_{i,n-1}. \tag{3.9}$$

Now Eq. (3.5) can be derived as:

$$\begin{aligned} Y_{i,j} \wedge Y_{j,n-1} &\Rightarrow X_{i,j} \wedge X_{j,n-1} \wedge X_{j,n} && \text{(from (3.2) and (3.8))} \\ &\Rightarrow (X_{i,j} \wedge X_{j,n-1}) \wedge (X_{i,j} \wedge X_{j,n}) \\ &\Rightarrow X_{i,n-1} \wedge X_{i,n} && \text{(from (3.6) and (3.7))} \\ &\Rightarrow Y_{i,n-1} && \text{(from (3.9)).} \end{aligned}$$

Note that the corresponding resolution proof will be of a fixed length – independent of n.

There are $O(n^2)$ clauses in F_{n-1} expressed over the Y variables and each is derived by a resolution proof of a fixed length similar to the derivation above. Thus, we require $O(n^2)$ resolutions to derive F_{n-1}. We proceed in this manner to derive F_3 which is then proved by resolution. We have thus shown:

Theorem 3.2. *For every n, there exists an extended resolution proof of F_n whose length is bounded by $c \cdot n^3$, where c is a fixed constant.*

We will now show that there exists polynomially bounded *symmetric resolution proofs* as well for F_n. Observe that F_n remains invariant under a permutation of $X_{i,j}$ induced by any permutation of the vertices 1, 2, ..., n. Thus, Σ_{F_n} is the group of permutations on the variables $X_{i,j}$ induced by the symmetric group on $\{1, 2, \ldots, n\}$.

Our symmetric resolution proof will imitate the following informal proof:

"Let us pick a vertex from $\{1, 2, \ldots, n\}$. Without loss of generality, assume it is n. (This is where the rule of symmetry will come into play.) Since n is not a source, there is an edge from some vertex to n, say from $n-1$. Continuing this argument we must either exhaust our vertex set, or come upon a cycle. In either case we arrive at a contradiction."

Observe that this is a distinctly different proof from the inductive argument used in the ER proof. While this argument is probably more natural, and the rule of symmetry is well-suited to capture this argument, an explanation of the SR proof seems to be somewhat tedious. So let us first outline the major steps involved in the SR proof:

1. Let A_n^k be the clause $\bigvee_{1 \leq i \leq k} X_{n,i}$. In Lemma 3.3 we prove $F_n \vdash_{\mathrm{SR}} A_n^{n-1}$.

2. F_n, $A_n^k \vdash_{\mathrm{SR}} A_n^{k-1}$ (Lemma 3.4). Together with Lemma 3.3, this implies that $F_n \vdash_{\mathrm{SR}} A_n'$, where $A_n' = X_{n,1}$.

3. By symmetry $X_{1,n}$ is derivable, yielding a contradiction. This is shown in Theorem 3.5. Further, we show that the length of this proof is $O(n^3)$.

Lemma 3.3. $F_n \vdash_{\mathrm{SR}} A_n^{n-1}$.

Proof. Consider F_{n-1}, the formula similar to F_n but written over the edges incident to the vertices $\{1, 2, 3, \ldots, n-1\}$. Clearly F_n contains $|F_{n-1}|$ clauses which are "super-clauses" of F_{n-1}. Call this set of clauses in F_n as $F_{n/n-1}$. The only variables in $F_{n/n-1}$ not present in F_{n-1} are $X_{n,i}$, $1 \leq i \leq n-1$. Recall that F_{n-1} is unsatisfiable. Hence, $F_{n-1} \vdash_{\mathrm{SR}} \square$. Since $F_{n/n-1}$ is a set of super-clauses of F_{n-1}, and since all the additional variables occur in the same parity, we can imitate the proof of $F_{n-1} \vdash \square$ into a proof of $F_{n/n-1} \vdash_{\mathrm{SR}} \bigvee_{1 \leq i \leq n-1} X_{n,i}$. A formal proof of this can be found in Lemma 5.8. Finally, since $F_{n/n-1}$ is a subset of F_n, we have shown that there exists a proof for $F_n \vdash_{\mathrm{SR}} A_n^{n-1}$ of the same length as the proof for $F_{n-1} \vdash \square$.

In the proof of the next Lemma, we use the following axioms from F_n:

$$\bar{X}_{n,k} \vee \bar{X}_{k,n}$$

$$\bar{X}_{n,k} \vee \bar{X}_{k,i} \vee X_{n,i} \quad \text{for } 1 \leq i < k.$$

(This is the CNF of $X_{n,k} \wedge X_{k,i} \Rightarrow X_{n,i}$.)

Lemma 3.4. F_n, $A_n^k \vdash_{SR} A_n^{k-1}$.

Proof. Recall that A_n^k is the clause $X_{n,1} \vee X_{n,2} \vee \ldots \vee X_{n,k}$. By the rule of symmetry, we can also derive $X_{k,1} \vee X_{k,2} \vee \ldots \vee X_{k,k-1} \vee X_{k,n}$. The derivation of A_n^{k-1} is indicated in Fig. 1. Observe that the length of this derivation is $O(n)$.

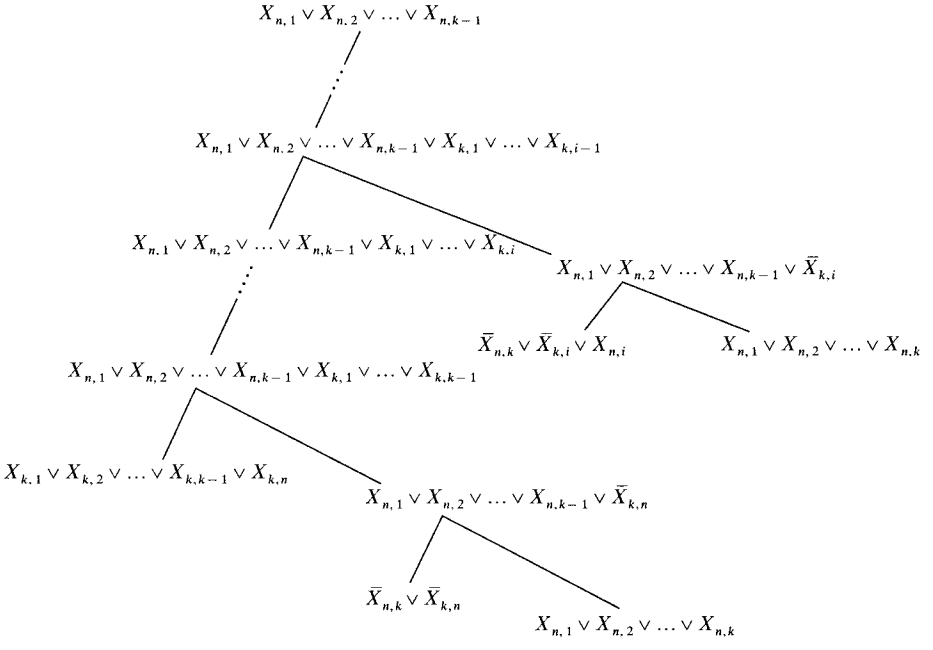

Fig. 1

Theorem 3.5. *For every n, there exists a symmetric resolution proof of F_n whose length is bounded by $c \cdot n^3$, where c is a fixed constant.*

Proof. Through one application of Lemma 3.3 and $O(n)$ applications of Lemma 3.4, we can derive $X_{n,1}$. By the rule of symmetry, we can derive $X_{1,n}$ (costing only one additional step). Then with the axiom $\bar{X}_{n,1} \vee \bar{X}_{1,n}$, we derive the empty clause. Let the length of this derivation be $f(n)$. We have shown

$$f(n) = f(n-1) + O(n) \cdot O(n).$$

Hence, $f(n)$ is $O(n^3)$ and the theorem follows.

We have shown that F_n, the statement asserting that an acyclic digraph on n vertices must have a source, has polynomially bounded extended resolution as well as symmetric resolution proofs. What makes these proofs interesting is the observation that without extension or symmetry, these statements appear to require exponentially long proofs under resolution. A number of other examples can be constructed along these lines. For example, we can encode the statement, "There is a perfect pairing of $2n+1$ elements", as:

$$\left[\bigwedge_{1 \leqq i \leqq 2n+1} \left(\bigvee_{\substack{1 \leqq j \leqq 2n+1 \\ i \neq j}} X_{i,j}\right)\right] \wedge \left[\bigwedge_{1 \leqq i < j < k \leqq 2n+1} (\bar{X}_{i,j} \vee \bar{X}_{i,k})\right]$$

where $X_{i,j}$ and $X_{j,i}$ are two representations of the same variable that stands for the proposition, "Elements i and j are paired." It can be shown that these unsatisfiable statements have polynomially bounded extended resolution and symmetric resolution proofs, while such short proofs are not known under plain resolution.

Cook's statements encoded from the pigeonhole principle [7] which have been shown to have short extended resolution proofs can also be shown to have short SR proofs.

4. Clever Arguments

We observe that the power of extension goes beyond imitating simple inductive arguments. In fact, extension allows the definition of intermediate hypotheses that can be introduced by defining new variables to stand for the hypotheses. A striking example arises from the checkerboard puzzle which asks if a checkerboard, two of whose diagonally opposite corner squares are removed, can be perfectly covered with dominoes.

Consider a $2n \times 2n$ square board with two of the diagonally opposite corner squares removed. We construct an unsatisfiable formula F_n on variables $X_{i,j}$ which stands for the statement: "There is a domino covering squares i and j." For each square in the pruned board, we write a formula that states: "Exactly one of the (at most) four dominoes that cover that square is present." F_n is then the conjunction of these formulas.

Formally, label each square of the pruned board with a unique integer i, $1 \leqq i \leqq 4n^2 - 2$. Define a propositional variable $X_{i,j}$ for every pair of squares i and j that are adjacent in the board. (For ease of notation, we will use $X_{i,j}$ as well as $X_{j,i}$ to mean the same variable.) For $1 \leqq i \leqq 4n^2 - 2$, let $S(i)$ be the set of indices of the squares adjacent to i. (Observe $|S(i)| \leqq 4$.) We are now ready to define the unsatisfiable formula:

$$B_n = \bigwedge_{1 \leqq i \leqq 4n^2-2} \{[\bigvee_{j \in S(i)} X_{i,j}] \wedge [\bigwedge_{j_1, j_2 \in S(i)} (\bar{X}_{i,j_1} \vee \bar{X}_{i,j_2})]\}.$$

Claim 4.1. For each $n \geqq 1$, B_n is unsatisfiable.

Proof. If we view the squares of the board to be colored with two colors, say black and white, like a checkerboard, the pruned board will have $2n^2$ squares of one color and $2n^2 - 2$ squares of the other. However, any satisfying assignment to B_n will pair up white squares with black squares. Clearly, this is not possible.

We will show a short ER proof for B_n. The ER proof will essentially encode the proof of Claim 4.1. Label the squares of the $2n \times 2n$ pruned board with two colors, black and white, like a checkerboard. Assume that the two diagonally opposite corner squares that have been removed would have been labelled black. Thus, the pruned board has $2n^2$ squares labelled whith and $2n^2 - 2$ squares labelled black.

Consider a fragment F of the board. Recall that the variables $X_{i,j}$ correspond to unit edges separating adjacent squares i and j of the board. Call a

variable $X_{i,j}$ as *internal* to the fragment F if both squares i and j are in the fragment F. Similarly, $X_{i,j}$ is said to be *external* to F if either i or j is in F, but not both. For example, in Fig. 2 dotted lines indicate external variables and solid lines indicate internal variables. (Double lines do not indicate variables since they are at the edge of the board and thus do not separate adjacent squares.)

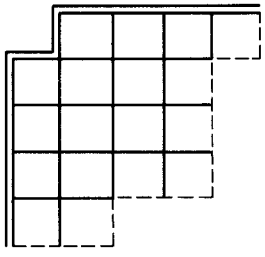

Fig. 2

Define F_{int} and F_{ext} to be the set of internal and external edges in F, respectively. For every $X_{i,j} \in F_{\text{ext}}$, exactly one of the squares i and j is present in F. Based on whether that square is white or black, partition F_{ext} into F^W_{ext} and F^B_{ext}, respectively. Define $\delta(F)$ as

$$\delta(F) = |\{i \in F \mid i \text{ is a white square}\}| - |\{i \in F \mid i \text{ is a black square}\}|.$$

Finally, for a set of variables θ, define $\|\theta\|$ as the number of $X \in \theta$ that are assigned TRUE under a specific truth assignment under consideration.

With this machinery we are ready to make an interesting observation:

Observation 4.2. For any satisfying assignment of truth values to the variables of B_n and any fragment F of the board,

$$\|F^W_{\text{ext}}\| - \|F^B_{\text{ext}}\| = \delta(F).$$

Proof. Very similar to the proof of Claim 4.1.

Observe that if F and $\bar{F}$ are complementary fragments, i.e., when merged they form the entire pruned board, then $F^W_{\text{ext}} = \bar{F}^B_{\text{ext}}$ and $F^B_{\text{ext}} = \bar{F}^W_{\text{ext}}$. Further,

$$\delta(F) + \delta(\bar{F}) = 2$$

$$\therefore \delta(F) = 2 - \delta(\bar{F}).$$

We will derive an ER proof from a sequence of fragments of the board. Beginning with individual squares as degenerate fragments, we will merge fragments to construct larger fragments. For each fragment F, we will define a new variable Z_F, a la the principle of extension. We will then show a derivation of Z_F. We will conclude by deriving Z_F and $Z_{\bar{F}}$ for two complementary fragments F and $\bar{F}$ and show that $Z_F \wedge Z_{\bar{F}}$ is a contradiction.

The main difficulty is in the definition of Z_F. We would like it to mean that Observation 4.2 is true for the fragment F. That is Z_F should represent the statement:

$$\text{“}\|F^W_{\text{ext}}\| - \|F^B_{\text{ext}}\| = \delta(F)\text{”}.$$

However, this requires an ability to count. For this purpose we define the functions $\Gamma_i(\theta, \Psi)$, where i is an integer (positive, negative or zero) and θ and Ψ are finite sets of variables. $\Gamma_i(\theta, \Psi)$ is defined inductively:

$$\Gamma_i(\emptyset, \emptyset) \equiv \begin{cases} \text{TRUE} & \text{if } i=0 \\ \text{FALSE} & \text{otherwise,} \end{cases}$$

$$\Gamma_i(\theta, \Psi \cup \{X\}) \equiv [(X \wedge \Gamma_{i+1}(\theta, \Psi)) \vee (\bar{X} \wedge \Gamma_i(\theta, \Psi))],$$

$$\Gamma_i(\theta \cup \{X\}, \Psi) \equiv [(X \wedge \Gamma_{i-1}(\theta, \Psi)) \vee (\bar{X} \wedge \Gamma_i(\theta, \Psi))].$$

Intuitively, $\Gamma_i(\theta, \Psi)$ is TRUE precisely when the number of variables in θ that are assigned TRUE minus the number of variables in Ψ that are assigned TRUE equals i.

Observe that $\Gamma_i(\theta, \Psi)$ can be defined in many ways by varying the order in which the variables of θ and Ψ are deleted. For purposes of computational efficiency, we will require that $\Gamma_i(\theta, \Psi)$ be defined through a fixed order of the variables in θ and Ψ. Choose any (arbitrary but fixed) order for the variables in the formula B_n. Since θ and Ψ will always be subsets of this set of variables, and since $\theta \cap \Psi$ will be necessarily empty, we can use this chosen order for defining $\Gamma_i(\theta, \Psi)$.

Let us first examine the complexity of the definition of $\Gamma_i(\theta, \Psi)$. Let $|\theta| + |\Psi| = k$. Let the sequence $\{(\theta_i, \Psi_i)\}_{i=1}^{k}$ be the pairs of sets obtained by deleting from θ or Ψ the appropriate variable one at a time. It can be shown by induction on k that to define $\Gamma_i(\theta, \Psi)$ we need to define the following intermediate variables:

For $1 \leqq j \leqq k$ and for $i - n_1 \leqq l \leqq i + n_2$, $\Gamma_l(\theta_j, \Psi_j)$, where $n_1(n_2)$ is the number of variables deleted from $\theta(\Psi)$ in the first j steps.

From the above observation, it is easily seen that since $n_1 + n_2$ always equals j, we need $\sum_{j=1}^{k} (j+1)$ additional variables to define $\Gamma_i(\theta, \Psi)$. Further, the defining equations for each variable can be represented by a fixed number of clauses. Hence, we claim:

Lemma 4.3. *Let θ and Ψ be sets of variables and $k = |\theta| + |\Psi|$. For $1 \leqq i \leqq k$, we can define $\Gamma_i(\theta, \Psi)$ with the introduction of $(k+1)(k+2)/2$ new variables and $O(k^2)$ clauses.*

Proof. By induction on $|\theta|$ and $|\Psi|$ as indicated above.

Recall that our objective is to define Z_F for a fragment F. We are ready to define it as:

$$Z_F \equiv \Gamma_{\delta(F)}(F_{\text{ext}}^W, F_{\text{ext}}^B).$$

Lemma 4.4. *Z_F can be defined by introducing at most $O(|F_{\text{ext}}|^2)$ new variables and clauses.*

Proof. Follows from Lemma 4.3 and the definition of Z_F.

Recall that our goal is to describe a short proof for B_n and our strategy is to consider a finite sequence of fragments $F_1, F_2, \ldots, F_m$ with the following properties:

a) F_m is the entire pruned board;

b) Each F_i is either a unit square of the board or is the union of two previous non-overlapping fragments.

We will show that for any fragment F corresponding to a unit square, Z_F is derivable from B_n and the defining equations for Z_F. This we do in Lemma 4.5. In Lemma 4.6 we show the corresponding inductive step leading to the derivation of the empty clause.

Lemma 4.5. *If F is a unit square, then there exists a proof for Z_F of a fixed length.*

Proof. Without loss of generality, assume that F is a white square with four adjacent squares – so that $|F_{\text{ext}}|=4$. By our assumption, $F^W_{\text{ext}}=F_{\text{ext}}$, $F^B_{\text{ext}}=\emptyset$, and $\delta(F)=1$. Thus, Z_F is defined as

$$Z_F \equiv \Gamma_1(F_{\text{ext}}, \emptyset).$$

By definition of the Γ functions, Z_F will be TRUE precisely when exactly one of the variables in F_{ext} is assgined TRUE. But that is exactly the axioms corresponding to F in B_n. Hence, with those axioms and the definitions of Z_F and the necessary Γ functions, we can derive Z_F. Finally, the length of this derivation is bounded since $|F_{\text{ext}}| \leqq 4$ for all F corresponding to unit squares.

Lemma 4.6. *Let F be a fragment of the board obtained as the union of two non-overlapping fragments G and H. Z_F can be derived from Z_G and Z_H, together with the definitions of Z_F, Z_G, and Z_H. Furthermore, the length of the derivation of Z_F is $O(k^3)$, where $k=|G_{\text{ext}}|+|H_{\text{ext}}|$.*

Proof. Recall that all the Γ functions use a fixed order of the variables for their definition. As per that order, let the elements of G_{ext}, H_{ext}, and F_{ext} be $g_1, g_2, \ldots, g_r$, $h_1, h_2, \ldots, h_s$, and $f_1, f_2, \ldots, f_t$, respectively. Since F is the union of G and H, F_{ext} consists of all elements in G_{ext} and H_{ext} that are not in both. That is,

$$F_{\text{ext}} = (G_{\text{ext}} \cup H_{\text{ext}}) - (G_{\text{ext}} \cap H_{\text{ext}}).$$

In addition, since G and H are non-overlapping, $\delta(F)=\delta(G)+\delta(H)$.

Consider the variables in $G_{\text{ext}} \cap H_{\text{ext}}$. It is easily seen that

$$G^W_{\text{ext}} \cap H^W_{\text{ext}} = G^B_{\text{ext}} \cap H^B_{\text{ext}} = \emptyset.$$

So,

$$G_{\text{ext}} \cap H_{\text{ext}} = (G^W_{\text{ext}} \cap H^B_{\text{ext}}) \cup (G^B_{\text{ext}} \cap H^W_{\text{ext}}).$$

That is, the variables common to G_{ext} and H_{ext} must lie on squares of opposite color.

We then observe that $f_1, f_2, \ldots, f_t$ is merely a merged listing of $g_1, g_2, \ldots, g_r$ and $h_1, h_2, \ldots, h_t$ with common elements omitted. Furthermore, when two elements are common, they lie in opposite colored partitions.

For the sake of concreteness, let $f_1=g_1$. That is, g_1 precedes h_1 in our chosen order and $g_1 \neq h_1$ – thus being the first element in the f-list. Consider

the following axioms obtained from the defining equations for Z_F, Z_G, and Z_H:

$$Z_G \equiv \Gamma_{\delta(G)}(G^W_{\text{ext}}, G^B_{\text{ext}}), \tag{4.1}$$

$$Z_F \equiv \Gamma_{\delta(F)}(F^W_{\text{ext}}, F^B_{\text{ext}}). \tag{4.2}$$

Now suppose $g_1 \in G^W_{\text{ext}}$. So, $g_1 \in F^W_{\text{ext}}$. We use the definitions:

$$\begin{aligned}\Gamma_{\delta(G)}(G^W_{\text{ext}}, G^B_{\text{ext}}) \equiv\ & g_1\, \Gamma_{\delta(G)-1}(G^W_{\text{ext}} - \{g_1\}, G^B_{\text{ext}}) \\ & \vee \bar{g}_1\, \Gamma_{\delta(G)}(G^W_{\text{ext}} - \{g_1\}, G^B_{\text{ext}}),\end{aligned} \tag{4.3}$$

$$\begin{aligned}\Gamma_{\delta(F)}(F^W_{\text{ext}}, F^B_{\text{ext}}) \equiv\ & g_1\, \Gamma_{\delta(F)-1}(F^W_{\text{ext}} - \{g_1\}, F^B_{\text{ext}}) \\ & \vee \bar{g}_1\, \Gamma_{\delta(F)}(F^W_{\text{ext}} - \{g_1\}, F^B_{\text{ext}}).\end{aligned} \tag{4.4}$$

Using Eqs. (4.1) thru (4.4), together with Z_G, we can derive

$$\begin{aligned}&([\Gamma_{\delta(G)-1}(G^W_{\text{ext}} - \{g_1\}, G^B_{\text{ext}}) \wedge \Gamma_{\delta(F)-1}(F^W_{\text{ext}} - \{g_1\}, F^B_{\text{ext}})] \\ &\quad \vee [\Gamma_{\delta(G)}(G^W_{\text{ext}} - \{g_1\}, G^B_{\text{ext}}) \wedge \Gamma_{\delta(F)}(F^W_{\text{ext}} - \{g_1\}, F^B_{\text{ext}})]) \Rightarrow Z_F.\end{aligned} \tag{4.5}$$

Observe that Eq. (4.5) expresses Z_F using Γ functions that do *not* depend on the variable g_1. We call this the elimination of variable g_1 (which is the same as f_1).

In this manner we eliminate each of the variables in the F-list. However, we will encounter situations where the leading variable in the F-list is not either of the leading variables in the G- or H-lists. This is because of variables in $G_{\text{ext}} \cap H_{\text{ext}}$ which, as explained earlier, are not in F_{ext}. Thus, in such situations, the leading variables in the G- and H-lists would be identical and in opposite colored partitions. We consider this as Case b of the general step explained below. Case a is the more common case where the leading element of the F-list is the leading element of either the G-list or the H-list, but not both.

Suppose that after eliminating a certain number of variables, G^W_{ext} and G^B_{ext} have been reduced to θ_G and Ψ_G. Similarly assume that H^W_{ext}, H^B_{ext}, F^W_{ext} and F^B_{ext} have been reduced to θ_H, Ψ_H, θ_F, and Ψ_F, respectively. Let l^W_F and l^B_F be the number of elements in F^W_{ext} and F^B_{ext} that have been eliminated. Similarly, define l^W_G, l^B_G, l^W_H, and l^B_H. Further, let l_G be the difference between the number of variables in G^W_{ext} and G^B_{ext} that are also in H_{ext} and have so far been eliminated. Similarly, define l_H.

Proceeding along the lines described for eliminating g_1, we will be able to derive

$$\bigvee_{\substack{\delta(G)-l_G-l^W_G \le l_1 \le \delta(G)-l_G+l^B_G \\ \delta(H)-l_H-l^W_H \le l_2 \le \delta(H)-l_H+l^B_H \\ \delta(F)-l^W_F \le l_1+l_2 \le \delta(F)+l^B_F}} (\Gamma_{l_1}(\theta_G, \Psi_G) \wedge \Gamma_{l_2}(\theta_H, \Psi_H) \wedge \Gamma_{l_1+l_2}(\theta_F, \Psi_F)) \Rightarrow Z_F. \tag{4.6}$$

The next variable to be eliminated could fall into one of two cases.

Case a. The variable occurs in the G-list or the H-list but not in both. In this case the next step of Eq. (4.6) can be derived. The length of this derivation would be proportional to the number of clauses representing (4.6).

Case b. The variable is common to the G- and H-lists. In this case the variable gets eliminated without any increase in the number of clauses representing the next step of (4.6). Once again the length of the derivation is proportional to the number of clauses needed to represent (4.6).

Proceeding in this manner we obtain the final step wherein θ_G, Ψ_G, θ_H, Ψ_H, θ_F, and Ψ_F are all empty. In the final version of Eq. (4.6) there will be a clause consisting solely of $\Gamma_0(\emptyset, \emptyset)$ function - which is identically TRUE, by definition. Hence that clause will derive Z_F.

To estimate the length of this derivation, we observe that there are $O(k)$ steps each of which is proportional to the length of Eq. (4.6). We must point out here that Eq. (4.6) can be represented in CNF without any significant increase in its length. Hence the length of Eq. (4.6) is $O(k^2)$.

The entire derivation of Z_F, therefore, requires at most $O(k^3)$ steps. That concludes the proof of the Lemma.

Theorem 4.7. *There exists ER proofs of B_n whose length is bounded by $c \cdot \omega^{2.5}$, where ω is the length of B_n.*

Proof. Using Lemma 4.5, Lemma 4.6, and the sequence of fragments F_1, $F_2, \ldots, F_m$, we can derive Z_{F_m} in $O(m \cdot k^3)$ steps, where m is the number of fragments and k is the size of the largest external set of variables of the fragments. Clearly we can choose $F_1, F_2, \ldots, F_m$ such that $m = O(n^2)$ and $k = O(n)$. Thus we can derive Z_{F_m} in $O(n^5)$ steps. Now,

$$Z_{F_m} \equiv \Gamma_{\delta(F_m)}(F^W_{m_{\text{ext}}}, F^B_{m_{\text{ext}}}).$$

But, $F_{m_{\text{ext}}} = \emptyset$ and $\delta(F_m) = 2$. Thus,

$$Z_{F_m} \equiv \Gamma_2(\emptyset, \emptyset)$$

which is, by the defining equations, FALSE. Hence we can derive the empty clause. Since these last steps are fixed in number, we have demonstrated a proof of B_n of length $O(n^5)$.

Now the length of B_n is $O(n^2)$. The theorem follows immediately.

In this section we have shown short ER proofs for the formulas B_n. It is natural to ask whether there are short SR or resolution proofs for B_n. We conjecture that a resolution proof for B_n is necessarily long. We briefly discuss the possibilities of constructing short SR proofs for B_n in Sect. 6.

In contrast to the results of this section, we present in the following section a set of unsatisfiable formulas for which there are short SR proofs - while short ER proofs are not currently known.

5. Non-Critical Ramsey Sentences

In [13] it has been pointed out that tautologies derived by asserting Ramsey's theorem are candidates for hard tautologies. The argument put forth is that no efficient procedure is currently known to demonstrate that a given number has a specific Ramsey property. However, weak upper bounds for Ramsey num-

bers have been established – in particular, in the course of the proof of Ramsey's theorem. We then observe that tautologies derived by asserting the Ramsey property of these upper bounds have short mathematical proofs. A natural question is to ask if these proofs can be encoded as short formal proofs in some suitable proof system. In this section we show a $O(m^{1+\varepsilon})$ SR proof for these tautologies, where m is the length of the tautologies and ε is a small positive number.

Recall (see [3]) that Ramsey's theorem asserts that for every pair of integers r_1, $r_2 \geqq 2$, there exists a sufficiently large positive integer n such that every graph on n vertices contains either a clique of size r_1 or an independent set of size r_2. In fact, it is shown in [3] that if $R(r_1, r_2)$ denotes the smallest n with the above property, then

$$R(r_1, r_2) \leqq R(r_1 - 1, r_2) + R(r_1, r_2 - 1).$$

Definition 5.1. Let

$$\hat{R}(r_1, r_2) = \hat{R}(r_1 - 1, r_2) + \hat{R}(r_1, r_2 - 1)$$

with

$$\hat{R}(2, r) = \hat{R}(r, 2) = r.$$

Claim 5.2. $\hat{R}(r_1, r_2)$ has the Ramsey property with parameters r_1 and r_2. That is, every graph on $\hat{R}(r_1, r_2)$ vertices contains either a clique of size r_1 or an independent set of size r_2.

Proof. An immediate consequence of Ramsey's theorem.

Definition 5.3. Let $n = \hat{R}(r_1, r_2)$ and $V_n = \{1, 2, \ldots, n\}$. For every pair of distinct vertices i and j, define a propositional variable $X_{i,j}$ representing the statement, "There is an edge between vertex i and vertex j." (Observe that, once again, $X_{i,j}$ and $X_{j,i}$ represent the same variable.) Define a formula $G(r_1, r_2)$ as

$$G(r_1, r_2) = [\bigwedge_{\substack{S \subset V_n \\ |S| = r_1}} (\bigvee_{i,j \in S} \bar{X}_{i,j})] \wedge [\bigwedge_{\substack{S \subset V_n \\ |S| = r_2}} (\bigvee_{i,j \in S} X_{i,j})].$$

Claim 5.4. For $r_1, r_2 \geqq 2$, $G(r_1, r_2)$ is unsatisfiable.

Proof. It is easily seen that $G(r_1, r_2)$ is the negation of Claim 5.2. Hence it is never satisfiable.

For the remainder of this section, let us fix $r_1, r_2 \geqq 2$ and $n = \hat{R}(r_1, r_2)$. We intend to demonstrate short SR proofs for $G(r_1, r_2)$. Observe that $\Sigma_{G(r_1, r_2)}$, the group of permutations that leave $G(r_1, r_2)$ invariant, is the set of edge permutations of the graph induced by all possible vertex permutation, i.e., the symmetric group on V_n.

We first define a set of clauses $\zeta^{A/a}_{B/b}$, where A and B are subsets of V_n and a and b are positive integers. $\zeta^{+}_{A/a \atop B/b}$ is the set of clauses obtained by selecting a vertices from the set A of vertices, b vertices from B and writing down the *positive* clique of size $a+b$ – asserting that there is at least one edge between the vertices of $A \cup B$. Similarly, we define $\zeta^{-}_{A/a \atop B/b}$. Formally,

Notation 5.5. Let A, $B \subseteq V_n$ (either A or B could be empty) and $a \leqq |A|$ and $b \leqq |B|$. Define

$$\zeta^{+}_{\substack{A/a \\ B/b}} = \{ \bigvee_{i,j \in S} X_{i,j} \}_{\substack{S = S_1 \cup S_2 \\ S_1 \subset A, S_2 \subset B \\ |S_1| = a, |S_2| = b}} .$$

Similarly, define

$$\zeta^{-}_{\substack{A/a \\ B/b}} = \{ \bigvee_{i,j \in S} \bar{X}_{i,j} \}_{\substack{S = S_1 \cup S_2 \\ S_1 \subset A, S_2 \subset B \\ |S_1| = a, |S_2| = b}} .$$

When either A or B is empty, we might omit it in the ζ notation, as in the following observation.

Observation 5.6. $G(r_1, r_2) = \zeta^{+}_{V_n/r_2} \cup \zeta^{-}_{V_n/r_1}$.

Proof. Easy.

Since the variables of G_r represent edges of a graph on the vertices V_n, a clause made up of these variables can be viewed as a graph. We then define a fan to be a clause whose graph is pictorially shown in Fig. 3.

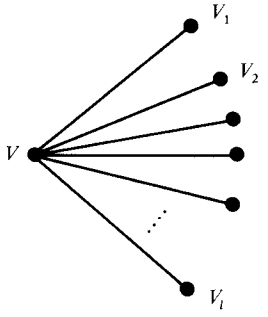

Fig. 3

Formally:

Notation 5.7. $F^{+}_{v \to \{v_1, v_2, \ldots, v_l\}}$ is the clause $(\bigvee_{1 \leqq i \leqq l} X_{v, v_i})$, where $v \in V_n$, $\{v_1, v_2, \ldots, v_l\} \subset V_n$ and, of course, $v \notin \{v_1, v_2, \ldots, v_l\}$. Similarly, we define $F^{-}_{v \to \{v_1, v_2, \ldots, v_l\}}$ as the clause $(\bigvee_{1 \leqq i \leqq l} \bar{X}_{v, v_i})$.

The next Lemma states an interesting property of resolution-style proof systems. If the axioms (clauses at the leaves) of a resolution proof tree are weakened by the introduction of additional literals (drawn from a new set of variables) such that no literal is introduced in both parities, the resulting tree is a legitimate resolution proof tree deriving a weaker clause – namely, the clause derived by the original tree together with the disjunction of all the new literals introduced in the axioms.

Lemma 5.8. *Let L be a set of literals such that no literal occurs in both parities. Let $\mathscr{B}$ be a set of clauses, C a clause, and $\mathscr{B} \vdash_R C$. Assume that no variable is common to both L and $\mathscr{B}$. For every $B \in \mathscr{B}$, let B' be a clause of the form $[B \vee (\bigvee_{l \in L_B} l)]$, where $L_B \subseteq L$. Let $\mathscr{B}'$ be the set of clauses B' derived from clauses*

in $\mathscr{B}$. Then, there exists a clause C', which depends on C, the set of axioms in $\mathscr{B}$ that is used in the derivation of C and the transformation from $\mathscr{B}$ to $\mathscr{B}'$ such that

i) $\mathscr{B}' \vdash_R C'$,

ii) *C' is of the form* $[C \vee (\bigvee_{l \in L_C} l)]$, *where* $L_C \subseteq L$.

Furthermore the length of the derivation of $\mathscr{B}' \vdash_R C'$ is at most the length of the derivation of $\mathscr{B} \vdash_R C$.

Proof. By induction on the height h of the proof tree for $\mathscr{B} \vdash_R C$.

Basis Step. For $h=0$, the derived clause C is, in fact, an axiom B in $\mathscr{B}$. By assumption there is a corresponding axiom B' in $\mathscr{B}'$ that meets the requirements for the desired clause C'. In addition B' depends only on B and the transformation $\mathscr{B} \to \mathscr{B}'$. The length of the derivation (which is 1) remains unchanged.

Inductive Step. Suppose the Lemma is true for all trees up to height $h-1$. Let there be a derivation for $\mathscr{B} \vdash_R C$ of height h. Consider the resolution at the root of the tree, as shown in Fig. 4. Suppose that C is obtained by resolving clauses C_1 and C_2 over the variable X. Let the subtrees commanded by C_1 and C_2 be T_1 and T_2, respectively. Since T_1 is of height $h-1$ or less, there is a derivation tree T_1' for a clause C_1' of the form $[C_1 \vee (\bigvee_{l \in L_{C_1}} l)]$. By the inductive hypothesis, the complexity of T_1', i.e., the number of distinct clauses in T_1', is at most the complexity of T_1. By a similar argument, we can construct a tree T_2' for a clause C_2' of the form $[C_2 \vee (\bigvee_{l \in L_{C_2}} l)]$.

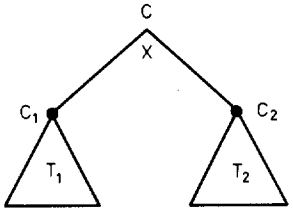

Fig. 4

Since the literals in C_1' and C_2' that are not present in C_1 and C_2 are all members of the set L, and since L does not contain literals in both parities, it follows that the only literals in C_1' that clash (are opposite in parity) with literals in C_2' are derived from C_1 and C_2. But X is the only clashing variable in C_1 and C_2. Hence X is the only clashing variable in C_1' and C_2'. Thus, C_1' and C_2' can resolve to give C'. It is easily seen that C' will be of the form $[C \vee (\bigvee_{l \in L_C} l)]$, where $L_C = L_{C_1} \cup L_{C_2} \subseteq L$.

We now need to show that the tree T' obtained from trees T_1' and T_2' (as shown in Fig. 5) is of complexity no greater than that of T. Since T_1' and T_2' have at most as many distinct clauses as T_1 and T_2, respectively, the only thing we need to show is that if a clause B occurs in both T_1 and T_2, then its transformed clauses B' and B'' in the two trees T_1' and T_2' are the same.

Observe that this may not be if the derivation for B in tree T_1 is different from the derivation for B in tree T_2. However, if we can ensure that clauses common to T_1 and T_2 have common derivations, then by the inductive hypothesis, the transformed clause will remain the same. We provide this assurance by starting with trees T_1'' and T_2'' instead of T_1 and T_2, wherein common clauses have common derivations. (Either of the two derivations can be chosen as the common one.)

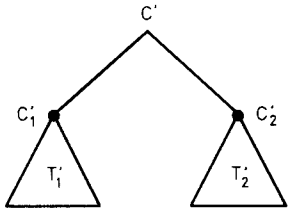

Fig. 5

Thus, if two clauses in the tree T' are distinct, the corresponding clauses in the tree T must have been distinct. In addition, it is easily seen that C' depends only on C, the axioms of T, and the transformation $\mathscr{B} \to \mathscr{B}'$.

That concludes the inductive step and the proof of the Lemma.

We are now ready to demonstrate a short SR proof for $G(r_1, r_2)$. Our strategy is to mimic the proof of Ramsey's theorem. We will construct a proof for $G(r_1, r_2)$ from proofs for $G(r_1 - 1, r_2)$ and $G(r_1, r_2 - 1)$. First, we show that $G(r, 2)$ and $G(2, r)$ have $O(r^2)$ proofs.

Lemma 5.9. *Let $m = |G(r, 2)|$. There exists an SR proof for $G(r, 2)$ of length at most $O(m)$. A similar result is also true for $G(2, r)$.*

Proof. Observe that $|G(r, 2)| = O(r^2)$ and that $G(r, 2)$ has $\binom{r}{2}$ clauses with a single literal and one clause of size $\binom{r}{2}$. It is easily seen from the composition of $G(r, 2)$ that there exists a resolution proof (the power of symmetry is not even needed) of length $\binom{r}{2}$. Clearly, a similar proof is valid for $G(2, r)$.

The next Lemma is the backbone of the short SR proof.

Lemma 5.10. *Suppose we have constructed proofs for $G(r_1 - 1, r_2)$ and $G(r_1, r_2 - 1)$. We can then construct an SR proof for $G(r_1, r_2)$ in $O(n^2)$ additional steps, where $n = \hat{R}(r_1, r_2)$.*

Proof. Select a set $A \subset V_n$ of size $\hat{R}(r_1 - 1, r_2)$ and a vertex $a \in V_n - A$. Since we have constructed a proof for $G(r_1 - 1, r_2)$, we can construct a similar proof for $G(r_1 - 1, r_2)$ specified over the vertices A. In other words, we can construct a proof for $[\zeta^+_{A/r_2} \cup \zeta^-_{A/r_1 - 1}] \vdash_R \square$ of length equal to the given proof for $G(r_1 - 1, r_2)$.

Observe that while ζ^+_{A/r_2} is a subset of $G(r_1, r_2)$, $\zeta^-_{A/r_1 - 1}$ is not a subset. This is because the "negative" clauses of $G(r_1, r_2)$ are of size $\binom{r_1}{2}$, while the clauses

of ζ^-_{A/r_1-1} are of size $\binom{r_1-1}{2}$. Nonetheless, $\zeta^-_{\substack{A/r_1-1\\ \{a\}/1}}$ is a subset of $G(r_1,r_2)$ and contains 'super-clauses" (in the spirit of Lemma 5.8) of ζ^-_{A/r_1-1}. So, by Lemma 5.8, we can construct a proof for

$$[\zeta^+_{A/r_2} \cup \zeta^-_{\substack{A/r_1-1\\ \{a\}/1}}] \vdash_R C$$

of length equal to the given proof for $G(r_1-1,r_2)$, where C is a clause containing literals in $\zeta_{\substack{A/r_1-1\\ \{a\}/1}}$ that are not in ζ^-_{A/r_1-1}. Clearly, the clause C is the fan $F^-_{a\to A}$.

Similarly, if B is a set of $\hat{R}(r_1,r_2-1)$ vertices not containing a, we can derive $F^+_{a\to B}$ by a proof whose length is at most that of $G(r_1,r_2-1)$.

Recall that V_n is the vertex set $\{1,2,\ldots,n\}$. Let $n_1=\hat{R}(r_1-1,r_2)$. By the principle of symmetry we can derive $F^-_{n\to\{1,2,\ldots,n_1\}}$. Further, since $n=\hat{R}(r_1-1,r_2)+\hat{R}(r_1,r_2-1)$, it follows that $\{n_1,n_1+1,\ldots,n-1\}$ is a set of $\hat{R}(r_1,r_2-1)$ vertices. Thus by the principle of symmetry we can derive $F^+_{n\to\{n_1,n_1+1,\ldots,n-1\}}$. Resolving these two fans we can get a clause

$$[F^-_{n\to\{1,2,\ldots,n_1-1\}} \vee F^+_{n\to\{n_1+1,\ldots,n-1\}}].$$

By repeated application of the principle of symmetry, we can derive $F^-_{n\to\{1,2,\ldots,n_1-1\}}$ as indicated in Fig. 6. The length of this derivation is clearly $O(n_1)$. We can similarly derive in $O(\hat{R}(r_1,r_2-1))$ resolutions the clause $F^+_{n\to\{1,2,\ldots,n_1-1\}}$. This way we have derived a fan of one smaller size. Proceeding thus, we can derive fans of smaller size and finally a fan of one literal. Two such complementary fans will complete the SR proof.

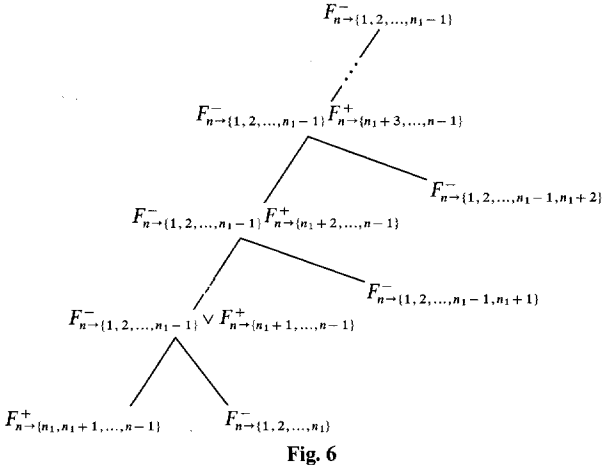

Fig. 6

Observe that the SR proof uses the proofs of $G(r_1-1,r_2)$ and $G(r_1,r_2-1)$. Hence the SR proof for $G(r_1,r_2)$ is $O(n^2)$ in addition to the sum of the lengths of the proofs for $G(r_1-1,r_2)$ and $G(r_1,r_2-1)$. That proves the lemma.

Theorem 5.11. *There exists SR proofs for $G(r_1,r_2)$ involving $O(n^4)$ symmetric resolution steps.*

Proof. Using Lemmas 5.9 and 5.10 we can construct a proof for every $G(i,j)$ $2 \leqq i \leqq r_1$, $2 \leqq j \leqq r_2$ in $O([\hat{R}(i,j)]^2)$ steps. That will then yield a proof for $G(r_1, r_2)$ in

$$\sum_{i,j} [\hat{R}(i,j)]^2 \leqq \sum_{i,j} [\hat{R}(r_1, r_2)]^2 \leqq n^4$$

steps. Observe that these steps are symmetric resolution steps.

It might seem paradoxical to prove a formula $(G(r_1, r_2))$ of length $\binom{n}{r_1} + \binom{n}{r_2}$ in n^4 steps for all r_1, r_2. However, it must be pointed out that each of the symmetric resolution steps requires the inspection of the entire formula to ensure that the chosen permutation leaves the formula invariant. This means that each of the SR steps is really $O(m)$ long, where m is the size of $G(r_1, r_2)$. Hence:

Corollary 5.12. *There exists SR proofs for $G(r_1, r_2)$ of length smaller than $O(m^{1+\varepsilon})$ for every $\varepsilon > 0$ provided r_1 and r_2 are sufficiently large.*

Proof. Clearly $m = \binom{n}{r_1} + \binom{n}{r_2}$. The proof that we have constructed has been shown to be of length $O(m \cdot n^4)$. Clearly, if r_1 and r_2 are sufficiently large, then n^4 grows slower than m^{ε} for a given $\varepsilon > 0$. Hence the proof.

We have shown an SR proof for $G(r_1, r_2)$ that closely follows the mathematical proof. This demonstrates the power of the principle of symmetry. Even though short ER proofs are not known for $G(r_1, r_2)$, we conjecture that there exist short ER proofs as well.

6. Concluding Remarks

In this paper we have demonstrated the use of the principles of extension and symmetry in encoding informal arguments as short formal proofs under the resolution proof system. As we had indicated in Sect. 1, the choice of the resolution proof system as the base proof system which is then augmented by the above two principles, is merely one of convenience. Cook and Reckhow [8] have shown that most reasonable proof systems, when augmented with the principle of extension, can polynomially simulate most other proof systems. Thus, similar succinct proofs such as those described in this paper can be demonstrated for other proof system such as Gentzen systems in conjunction with extension. Consequently, the principles of extension and symmetry are interesting proof rules in their own right.

In Sect. 3 we indicated that some inductive arguments could well be captured in either ER or SR. Recent results due to Haken [11] have shown that some of these classes of tautologies have *no polynomial length proofs* under ordinary resolution. However, his results exploit the fact that these tautologies include large clauses (i.e., $O(n^c)$, where n is the number of variables), in their conjunctive normal form. If one were to convert these tautologies to 3-CNF, these large clauses would disappear, and it is not clear that Haken's proof would carry through. Thus, the complexity of resolution when restricted to 3-CNF formulas remains an open problem.

In Sect. 4 we provided the details of a short ER proof for the formulas B_n derived from the checkerboard puzzle. We showed how ER could imitate the clever informal proof for the validity (or more precisely, the absurdity) of B_n. This illustration of the power of extension differs from previous demonstrations of a similar nature. Tseitin's original demonstration [16] uses tautologies that involve biconditionals. However, Dunham and Wang [9] have shown that one can construct short proofs for those tautologies in a suitable proof system, without the use of extension. Cook's demonstration for the use of extension [7], which we have applied to other inductive arguments in Sect. 3, makes use of extension in a limited sense. In fact, Reckhow [14] has formalized this restricted use of extension, as *limited extension*, wherein the definitions for the introduction of new variables are required to be sub-formulas of the original tautology. In contrast to these examples, the checkerboard example introduces intermediate variables that stand for lemmas. And, in particular, these lemmas are not merely sub-formulas of the original tautology. In that sense, this is a more powerful demonstration of the use of the principle of extension.

It is natural to ask if SR could also yield short proofs for B_n. Let us consider the group of invariance Σ_{B_n}. It consists of permutations of the variables induced by permutations of the squares of the board that leave the board "invariant." Clearly, every such permutation must be a rotation/reflection of the board and there are only four permutations that leave the board unchanged: 0° and 180° rotations of the board and the reflections about the two diagonals. This means that $|\Sigma_{B_n}|=4$. It is easy to see that the complexity of a resolution proof for a formula F is at most $|\Sigma_F|$ times the complexity of an SR-I proof for the same formula. Thus, SR-I proofs for B_n will not be significantly shorter than resolution proofs for B_n. Since we have conjectured that resolution proofs for B_n are necessarily long (Sect. 4), we should not expect short SR-I proofs either.

On the other hand, SR-II might prove appreciably more powerful in this case. The board possesses abundant local symmetry which could be used to advantage by an SR-II proof. However, more concrete claims on the lengths of SR-II proofs for B_n must await further investigation. On a similar note, Tseitin's axamples (see [16]) possess similar symmetry which SR-I might fail to exploit, whereas SR-II might prove more useful.

The formulas $\{B_n\}$ also seem to be good candidates for establishing exponential complexity for regular resolution using techniques similar to Tseitin's. Such a result would prove very useful and might also lend itself more readily to modifications of the sort suggested in [2]. However, there is presently no evidence to suggest that results more powerful than Tseitin's can be obtained through the use of B_n.

In Sect. 5 we showed that a powerful mathematical theorem, such as Ramsey's theorem, can be established succinctly within the framework of the resolution proof system in conjunction with the principle of symmetry. Furthermore, the ease with which these proofs can be demonstrated, makes the principle of symmetry very attractive.

We could have defined the concept of symmetry to include complementation. In that case for a formula F on n variables, we would consider the group $\Sigma_F \times \{0,1\}^n$. This would permit the mapping of literals to literals instead

of variables to variables, and ensure that the literals are mapped consistently. This would lead to C-symmetric resolution proof systems, CSR-I and CSR-II.

We might ask if, in fact, symmetry can be simulated through extension. (Observe that it is unlikely that extension could be simulated through symmetry, since a formula might have no symmetry whatsoever and yet would be amenable to extension.) One plausible approach is to use Cook's results detailed in [6]. He defines a system called PV for number theory and suggests that a theorem is provable in PV iff it is p-verifiable, i.e., there is a polynomially bounded uniform procedure to verify the validity of every instance of that theorem. He then defines a proof system for the propositional calculus to be p-verifiable if every step of the proof can be verified by a polynomially bounded uniform procedure. He shows that ER is p-verifiable and, in addition, that ER can polynomially simulate every p-verifiable proof system.

Under this notion it is not clear if SR is p-verifiable. If it is, then by Cook's results ER can p-simulate SR. On the other hand, if SR is not p-verifiable, then SR is in some sense independent of ER. We can then construct combinations of extension and symmetry. Depending on whether symmetry is allowed to operate on extended variables or not, we get two systems: SER and ESR. The power of these proof systems remains unexplored.

In any case the principle of symmetry provides a very convenient proof system to capture informal mathematical arguments as formal proofs. Even if extension were to subsume symmetry, SR might prove an easier proof system to work with in certain cases. For example, the non-critical Ramsey sentence G_r is a case in point.

Finally, the motivation for studying the lengths of proofs comes from the open problem: "Is NP closed under complementation?" If it is not, as is commonly believed, the complement of an NP-complete set is not in NP. Thus, the set of all unsatisfiable formulas in the propositional calculus – being the complement of the NP-complete set SAT – would not be in NP. This would indicate that there are unsatisfiable formulas (and correspondingly, tautologies as well) that do not have short proofs in any proof system. Even though establishing even exponential complexity results for such proof systems as resolution would fall far short of settling this open problem, it would add avidence to the conjecture that NP is not closed under complementation.

The results of this paper (indicating short proofs for tricky formulas) should not be interpreted as an attempt to refute this conjecture. Instead it is an attempt to study the limitations of powerful proof systems such as ER and SR by precisely capturing their power.

It is our view that any attempts to establish lower bound results on the complexity of super proof systems must address ER and SR. However, non-trivial lower bounds for such proof systems must await significant advances on similar questions about more modest proof systems such as resolution.

Acknowledgements. I would like to thank Robbie Moll for the many stimulating discussions on these and related topics. Thanks are also due to Rick Statman and Shelly Akers for the helpful discussions I had with them and to Lisa Wilson for her typing assistance during the many revisions of this paper.

References

1. Bauer, M., Brand, D., Fischer, M.J., Meyer, A.R., Paterson, M.S.: A Note on Disjunctive Form Tautologies. SIGACT News **5**, 17–20 (1973)
2. Ben-ari, M.: A Simplified Proof That Regular Resolution is Exponential. Inf. Process. Lett. **10**, 96–98 (1980)
3. Bondy, J.A., Murty, U.S.R.: Graph Theory with Applications. New York: North Holland 1979
4. Chang, C.L., Lee, R.C.T.: Symbolic Logic and Mechanical Theorem Proving. New York: Academic Press 1973
5. Cook, S.A.: The Complexity of Theorem Proving Procedures. Proc. of the Third Annual ACM Symp. on Th. of Computing pp. 151–158 (1971)
6. Cook, S.A.: Feasibily Constructive Proofs in the Propositional Calculus. Proc. of the Seventh Annual ACM Symp. on Th. of Computing pp. 83–97 (1975)
7. Cook, S.A.: A Short Proof on the Pigeon-hole Principle Using Extended Resolution. SIGACT News **8**, 28–32 (1976)
8. Cook, S.A., Reckhow, R.A.: The Relative Efficiency of Propositional Proof Systems. J. Symb. Logic **44**, 36–50 (1979)
9. Dunham, B., Wang, H.: Towards Feasible Solutions of the Tautology Problem. Ann. Math. Logic **10**, 117–154 (1976)
10. Galil, Z.: The Complexity of Resolution Procedures for Theorem Proving in the Propositional Calculus. Ph.D. Thesis, Dept. of Computer Science, Cornell University, 1975
11. Haken, A.: The Intractability of Resolution. Ph.D. Thesis, University of Illinois at Urbana-Champaign, 1984
12. Kleene, S.: Mathematical Logic. New York: Wiley 1967
13. Krishnamurthy, B., Moll, R.N.: Examples of Hard Tautologies in the Propositional Calculus. Proc. of the Thirteenth ACM Symp. on Th. of Computing pp. 28–37 (1981)
14. Reckhow, R.A.: On the Lengths of Proofs in the Propositional Calculus. Ph.D. Thesis, Dept. of Computer Science, University of Toronto, 1976
15. Robinson, J.A.: A Machine Oriented Logic Based on the Resolution Principle. J. ACM **12**, 23–41 (1965)
16. Tseitin, G.S.: On the Complexity of Derivations in Propositional Calculus. In: Structures in Constructive Mathematics and Mathematical Logic, II. A.O. Slisenko (ed.), pp. 115–125, 1968

Received September 27, 1983/March 13, 1985