THE JOURNAL OF SYMBOLIC LOGIC
Volume 52, Number 4, Dec. 1987

POLYNOMIAL SIZE PROOFS OF THE PROPOSITIONAL PIGEONHOLE PRINCIPLE

SAMUEL R. BUSS

Abstract. Cook and Reckhow defined a propositional formulation of the pigeonhole principle. This paper shows that there are Frege proofs of this propositional pigeonhole principle of polynomial size. This together with a result of Haken gives another proof of Urquhart's theorem that Frege systems have an exponential speedup over resolution. We also discuss connections to provability in theories of bounded arithmetic.

§1. Introduction. The motivation for this paper comes primarily from two sources. First, Cook and Reckhow [2] and Statman [7] discussed connections between lengths of proofs in propositional logic and open questions in computational complexity such as whether $NP = \text{co-}NP$. Cook and Reckhow used the propositional pigeonhole principle as an example of a family of true formulae which had polynomial size proofs in an extended Frege system and for which the only known proofs in Frege systems (i.e. the usual Hilbert style propositional logic) were exponential size. The main result of this paper is that the propositional pigeonhole principle also has polynomial size Frege proofs, contrary to expectations. On the other hand, Haken [4] has shown that any resolution proof of the propositional pigeonhole principle must be of exponential size. It follows that a Frege proof system has an exponential speedup over resolution (this was originally proved by Urquhart [11] with a different set of formulae).

The second motivation is from research in theories of bounded arithmetic. Alan Woods [10] showed that $I\Delta_0$ could prove the existence of an infinite number of primes if it were the case that $I\Delta_0$ could prove the pigeonhole principle for functions definable by a bounded formula. Alex Wilkie [9] discovered that a weak form of the pigeonhole principle is provable in $I\Delta_0 + \Omega_1$ and that this implies that $I\Delta_0 + \Omega_1$ can prove the existence of an infinite number of primes; however, it is still open whether $I\Delta_0 + \Omega_1$ proves the usual version of the pigeonhole principle for functions defined by bounded formulae. This question is related to the size of Frege proofs of the propositional pigeonhole principle by a result of Paris and Wilkie [5]; namely, if $I\Delta_0$ proves a relativized version of the pigeonhole principle then there are constant formula-depth, polynomial size Frege proofs of the propositional pigeonhole

Received July 4, 1986.
Research supported in part by NSF postdoctoral fellowship DMS85-11465 and by the Mathematical Sciences Research Institute.

0022-4812/87/5204-0003/$02.20

principle. We show below that under some additional assumptions, the converse of Paris and Wilkie's theorem holds too.

The first and main part of this paper proves the existence of short Frege proofs of the propositional pigeonhole principle. This proof is self-contained and elementary. The second part discussed connections with bounded arithmetic and presupposes knowledge of earlier research.

§2. Propositional proof systems. We begin by reviewing some definitions and constructions of Cook and Reckhow [2]. A *propositional formula* is constructed from propositional variables $p, q, r, \ldots$, which are interpreted as ranging over the truth values "True" and "False", and from propositional unary and binary connective such as $\neg$ (not), $\wedge$ (and), $\vee$ (or) and $\rightarrow$ (implication). A *Frege system* is a Hilbert-style propositional proof system for reasoning with propositional formulae. For the sake of definiteness, we shall let the Frege system $\mathscr{F}$ have propositional connectives $\neg$, $\wedge$, $\vee$, and $\rightarrow$, and the following 13 axioms:

$$
\begin{array}{ll}
\varphi \rightarrow \psi \rightarrow \varphi \wedge \psi, & \varphi \rightarrow \psi \rightarrow \varphi, \\
\varphi \wedge \psi \rightarrow \varphi, & \neg\varphi \rightarrow \varphi \rightarrow \psi, \\
\varphi \wedge \psi \rightarrow \psi, & (\varphi \rightarrow \psi \rightarrow \chi) \rightarrow (\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \chi), \\
\varphi \rightarrow \varphi \vee \psi, & (\varphi \rightarrow \chi) \rightarrow (\psi \rightarrow \chi) \rightarrow (\varphi \vee \psi \rightarrow \chi), \\
\psi \rightarrow \varphi \vee \psi, & (\varphi \rightarrow \psi \rightarrow \chi) \rightarrow (\psi \rightarrow \varphi \rightarrow \chi), \\
\neg\neg\varphi \rightarrow \varphi, & (\varphi \rightarrow \psi) \rightarrow (\neg\psi \rightarrow \neg\varphi), \\
\varphi \rightarrow \neg\neg\varphi; &
\end{array}
$$

and as its only rule, modus ponens; namely, from φ and $\varphi \rightarrow \psi$ infer ψ. In the axioms and the rule, any propositional formulae may be substituted for φ, ψ and χ. We follow the usual conventions concerning parentheses and the precedence of operations; namely, $\neg$ has highest precedence, $\rightarrow$ has the lowest and associates from right to left, so $\varphi \rightarrow \psi \rightarrow \chi$ means $\varphi \rightarrow (\psi \rightarrow \chi)$. A *Frege proof*, or for short an $\mathscr{F}$-proof, is a sequence $A_1, \ldots, A_n$ of propositional formulae such that each A_i either is an axiom or follows by modus ponens from some A_j and A_k with $j, k < i$. The last formula A_n is the conclusion of the proof.

There are two common notions of the length of a proof. The first is the number of formulae appearing in the proof, which is often called the number of *lines* or number of *inferences* of the proof. The second and, in our opinion, more relevant notion is the total number of symbols appearing in the proof. To count the total number of symbols, we shall assume that the propositional variables p_i are written as a "p" followed by digits in base 10 (say). So $p108$ denotes p_{108}. Thus proofs are written as a string in a finite alphabet containing, $p, 0, \ldots, 9$, $\wedge$, $\vee$, $\neg$, $\rightarrow$, (,) and comma; the *size* of a proof is defined to be the total number of symbols in the proof. It is an important property of Frege systems that the sizes of proofs in two different Frege systems are polynomially related: if $\mathscr{F}_1$ and $\mathscr{F}_2$ are Frege systems then there exists a polynomial q such that if A is a formula in the language of $\mathscr{F}_1$ and $\mathscr{F}_2$ and A has an $\mathscr{F}_1$-proof of size n then A has an $\mathscr{F}_2$-proof of size less than $q(n)$. Or, in Cook and Reckhow's terminology, any two Frege systems can p-simulate each other.

The *size* of a formula is defined to be the total number of symbols appearing in the formula.

An *extended Frege proof system* is a Frege system enhanced to allow the introduction of abbreviations. Any two extended Frege systems can p-simulate each other, so our work applies to any extended Frege system. For the sake of definiteness, we define the extended Frege system e$\mathscr{F}$ to have the language, axioms and rules of $\mathscr{F}$ plus a new rule called the *extension rule*. (The extension rule was originally defined by Tseĭtin [8].) A sequence of formulae $A_1, \ldots, A_n$ is an e$\mathscr{F}$-proof iff each A_i is an axiom or is deduced by modus ponens or by the extension rule. A_i is deduced by the extension rule iff A_i is of the form $(p_i \to B) \wedge (B \to p_i)$ where the propositional variable p_i does not appear in $A_1, \ldots, A_{i-1}$, A_n or B. The *size* of an extended Frege system is again defined to be the number of symbols in the proof; however, in this case, there is a polynomial p such that, for any e$\mathscr{F}$-proof containing n formulae, there is an e$\mathscr{F}$-proof with the same conclusion and with size less than $p(n)$. Thus for our purposes, the distinction between the size of an e$\mathscr{F}$-proof and the number of formulae in it are unimportant (Statman [7]).

An important open problem is whether $\mathscr{F}$ p-simulates e$\mathscr{F}$, i.e., whether there is a polynomial q such that for any e$\mathscr{F}$-proof of size n, there is an $\mathscr{F}$-proof of size less than $q(n)$ with the same conclusion. The natural conjecture is that any function q with this property must have growth rate similar to the exponential function.

§3. The propositional pigeonhole principle. For each natural number $n > 1$, we let PHP_n be a propositional formula expressing the principle that "if $n + 1$ pigeons sit in n holes then some hole contains more than one pigeon". More formally, let $[n]$ be the set $\{0, 1, \ldots, n - 1\}$; then if $f\colon [n + 1] \to [n]$ then there are $0 \le i < j \le n$ such that $f(i) = f(j)$. To express this propositionally, we let $p_{i,j}$ be propositional variables signifying $f(i) = j$ and define PHP_n to be the formula

$$\bigwedge_{0 \le i \le n} \bigvee_{0 \le j < n} p_{i,j} \to \bigvee_{0 \le i < m \le n} \bigvee_{0 \le j < n} (p_{i,j} \wedge p_{m,j}).$$

The symbols $\bigwedge$ and $\bigvee$ are shorthand notation for writing out a long string of conjunctions or disjunctions respectively. It is easy to see the left-hand side expresses the fact that f is total (perhaps multivalued) and the right-hand side that f is not one-to-one. Note that the size of PHP_n is proportional to n^3.

In [2], Cook and Reckhow showed that PHP_n has polynomial sized e$\mathscr{F}$-proofs; since it is an instructive example, we review it here. The idea of the proof is to define $f_n = f$ and f_i from f_{i+1} so that

$$f_i(x) = \begin{cases} f_{i+1}(x) & \text{if } f_{i+1}(x) \ne i, \\ f_{i+1}(i + 1) & \text{otherwise.} \end{cases}$$

Then it is easy to see by induction on i varying from n to 1 that if $f\colon [n + 1] \to [n]$ is one-to-one, then $f_i\colon [i + 1] \to [i]$ is one-to-one. In other words, we see that $\neg\mathrm{PHP}_{i+1} \to \neg\mathrm{PHP}_i$; hence $\neg\mathrm{PHP}_n \to \neg\mathrm{PHP}_1$. But PHP_1 is obviously true; hence PHP_n is valid.

To formalize this proof in the extended Frege system e$\mathscr{F}$, we use new propositional variables $q^k_{i,j}$ which represent the assertion that $f_k(i) = j$. To do this, we use the extension rule to define

$$q^n_{i,j} \leftrightarrow p_{i,j}, \qquad 0 \le i \le n, 0 \le j < n,$$
$$q^k_{i,j} \leftrightarrow q^{k+1}_{i,j} \vee (q^{k+1}_{i,k} \wedge q^{k+1}_{k+1,j}), \qquad 0 \le i \le k, 0 \le j < k, 1 \le k < n.$$

Let A_k be the propositional formula

$$\bigwedge_{0 \le i \le k} \bigvee_{0 \le j < k} q^k_{i,j} \to \bigvee_{0 \le i < m \le k} \bigvee_{0 \le j < k} q^k_{i,j} \wedge q^k_{m,j}.$$

Then it is clear that there are e$\mathscr{F}$-proofs of $\neg \mathrm{PHP}_n \to \neg A_n$ and $\neg A_{k+1} \to \neg A_k$ for all $1 \le k < n$ and such that each proof has size $O(n^6)$. This size estimate is obtained by seeing that there is an e$\mathscr{F}$-proof of $\neg A_{k+1} \to \neg A_k$ with $O(n^3)$ lines and each formula in this proof has size $O(n^3)$. Since A_1 is just $q^1_{0,0} \wedge q^1_{1,0} \to q^1_{0,0} \wedge q^1_{1,0}$ there is an e$\mathscr{F}$-proof of A_1. Hence by using modus ponens n times the e$\mathscr{F}$-proofs of $\neg \mathrm{PHP}_n \to \neg A_n$ and $\neg A_{k+1} \to \neg A_k$ combine to give an e$\mathscr{F}$-proof of PHP_n of size $O(n^7)$.

There is a simple way to convert this e$\mathscr{F}$-proof of PHP_n into an $\mathscr{F}$-proof; namely, replace each propositional variable introduced by the extension rule by the formula it abbreviates. Let $Q^k_{i,j}$ be inductively defined by

$$Q^n_{i,j} = p_{i,j} \quad \text{and} \quad Q^k_{i,j} = Q^{k+1}_{i,j} \vee (Q^{k+1}_{i,k} \wedge Q^{k+1}_{k+1,j}),$$

and replace each occurrence of $q^k_{i,j}$ in the e$\mathscr{F}$-proof by $Q^k_{i,j}$. The result is easily converted into an $\mathscr{F}$-proof of PHP_n with about the same number of lines as the e$\mathscr{F}$-proof. However, the size of the formulae $Q^1_{0,0}$ and $Q^1_{1,0}$ is about 3^n; hence the size of the $\mathscr{F}$-proof is $O(n^4 \cdot 3^n)$.

This example was used by Cook and Reckhow to illustrate how extended Frege systems are apparently more efficient than Frege systems in terms of proof size. However this is no longer a good example, since we show below that the propositional pigeonhole principle does indeed have polynomial size Frege proofs. It would be desirable to show that $\mathscr{F}$ is exponentially less efficient than e$\mathscr{F}$; our work merely shows that the propositional pigeonhole principle does not separate $\mathscr{F}$ from e$\mathscr{F}$ in this way.

§4. The polynomial size proof. The strategy for proving the existence of a short $\mathscr{F}$-proof of PHP_n will be to show that for some constants $r, s \in \mathbf{N}$ there is an e$\mathscr{F}$-proof of PHP_n of size $O(n^r)$ such that the propositional variables introduced by the extension rule abbreviate formulae of size $O(n^s)$. The first task is to show that there are such proofs for handling facts about counting and addition.

DEFINITION. We let $A \leftrightarrow B$ abbreviate $(A \to B) \wedge (B \to A)$ and $A \oplus B$ abbreviate $(A \wedge \neg B) \vee (\neg A \wedge B)$. So $\leftrightarrow$ denotes equivalence and $\oplus$ denotes the exclusive or.

DEFINITION. Let $\rho \ge 1$ and suppose $\varphi^l_0, \ldots, \varphi^l_\rho$ $(0 \le l \le 2)$ are propositional formulae. We define $\mathrm{Add}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2)$ to be the conjunction of the following formulae (where $1 \le i \le \rho$):

$$\varphi^0_0 \leftrightarrow \varphi^1_0 \oplus \varphi^2_0,$$

$$\varphi^0_i \leftrightarrow \varphi^1_i \oplus \varphi^2_i \oplus \bigvee_{0 \le j < i} \left(\varphi^1_j \wedge \varphi^2_j \wedge \bigwedge_{j < k < i} (\varphi^1_k \oplus \varphi^2_k) \right).$$

We follow the convention that an empty disjunction, say $\bigvee\!\!\!\bigvee_{0 \le j < i} A_j$ with $i = 0$, is always false and an empty conjunction always true. This can be done by defining any empty disjunction to be $(p_0 \wedge \neg p_0)$ and any empty conjunction to be $(p_0 \vee \neg p_0)$.

The purpose of defining Add_ρ is that when we let $x_i^l = 1$ if φ_i^l is true and $x_i^l = 0$ otherwise and define $n^l = \Sigma_i 2^i \cdot x_i^l$ then $\mathrm{Add}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2)$ asserts that n^0 is the sum of n^1 and n^2 modulo $2^{\rho+1}$. This is easily seen once it is noted that

$$\bigvee\!\!\!\bigvee_{0 \le j < i} \left(\varphi_j^1 \wedge \varphi_j^2 \wedge \bigwedge\!\!\!\bigwedge_{j < k < i} (\varphi_k^1 \oplus \varphi_k^2) \right)$$

is true if and only if there is a carry into the ith position of the sum.

Definition. Let m be a natural number. We let $\bar{m}$ denote the vector of propositional formulae $\psi_0, \psi_1, \ldots, \psi_\rho, \ldots$ such that if $\bar{m}$ has binary expansion $\Sigma_i 2^i \cdot m_i$ then for all i, if $m_i = 0$ then ψ_i is the formula $(p_0 \wedge \neg p_0)$ and if $m_i = 1$ then ψ_i is $(p_0 \vee \neg p_0)$. Thus the propositional formulae $\bar{m}$ represent the constant m.

Lemma 1. *Suppose $\varphi_0^l, \ldots, \varphi_\rho^l$ for $l = 1, 2$ are propositional formulae. Let $\varphi_0^0, \ldots, \varphi_\rho^0$ be the natural propositional formulae such that* $\mathrm{Add}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2)$ *holds. Let m be the maximum size of the φ_i^1's and the φ_i^2's. Then the size of each φ_i^0 is less than $c\rho^2 m$, where c is a fixed constant* (*independent of ρ and m*).

Proof. This is clear by inspection. ■

The reason Lemma 1 is important to us is that we will shortly be describing extended Frege proofs in which, for formulae $\varphi_0^1, \varphi_0^2, \ldots, \varphi_\rho^1, \varphi_\rho^2$, the extension rule is used to introduce new variables $q_0, \ldots, q_\rho$ for which $\mathrm{Add}_\rho(\vec{q}, \vec{\varphi}^1, \vec{\varphi}^2)$ is valid. Size estimates of the type given in Lemma 1 will help to determine how large the formula and proof sizes grow when the extended Frege proof is translated into a Frege proof by expanding the abbreviations introduced by the extension rule.

Definition. Let $\rho \ge 0$ and suppose $\varphi_0^l \ldots, \varphi_\rho^l$ are propositional formulae for $l = 0, 1$. We define the propositional formulae EQ_ρ, Less_ρ, and LE_ρ by

$$\mathrm{EQ}_\rho(\vec{\varphi}^0, \vec{\varphi}^1) \equiv \bigwedge\!\!\!\bigwedge_{0 \le i \le \rho} (\varphi_i^0 \leftrightarrow \varphi_i^1),$$

$$\mathrm{Less}_\rho(\vec{\varphi}^0, \vec{\varphi}^1) \equiv \bigvee\!\!\!\bigvee_{0 \le i \le \rho} \left(\neg \varphi_i^0 \wedge \varphi_i^1 \wedge \bigwedge\!\!\!\bigwedge_{i < j \le \rho} (\varphi_j^0 \leftrightarrow \varphi_j^1) \right),$$

$$\mathrm{LE}_\rho(\vec{\varphi}^0, \vec{\varphi}^1) \equiv \mathrm{EQ}_\rho(\vec{\varphi}^0, \vec{\varphi}^1) \vee \mathrm{Less}_\rho(\vec{\varphi}^0, \vec{\varphi}^1).$$

So the formulae EQ_ρ, Less_ρ and LE_ρ assert that the number coded by $\vec{\varphi}^0$ is equal to, less than, or not greater than (respectively) the number coded by $\vec{\varphi}^1$.

Lemma 2. *Let q_i^l and r_i^l be propositional variables for $0 \le i \le p$, $0 \le l \le 2$. Then there are Frege proofs of*

(a) $\mathrm{Add}_\rho(\vec{q}^0, \vec{q}^1, \vec{q}^2) \wedge \mathrm{Add}_\rho(\vec{r}^0, \vec{q}^2, \vec{q}^1) \rightarrow \mathrm{EQ}_\rho(\vec{q}^0, \vec{r}^0)$,

(b) $\mathrm{LE}_\rho(\vec{q}^1, \vec{r}^1) \wedge \mathrm{LE}_\rho(\vec{q}^2, \vec{r}^2) \wedge \neg r_\rho^1 \wedge \neg r_\rho^2 \wedge \mathrm{Add}_\rho(\vec{q}^0, \vec{q}^1, \vec{q}^2) \wedge \mathrm{Add}_\rho(\vec{r}^0, \vec{r}^1, \vec{r}^2) \rightarrow \mathrm{LE}_\rho(\vec{q}^0, \vec{r}^0)$,

(c) $\mathrm{LE}_\rho(\vec{q}^1, \vec{r}^1) \wedge \mathrm{Less}_\rho(\vec{q}^2, \vec{r}^2) \wedge \neg r_\rho^1 \wedge \neg r_\rho^2 \wedge \mathrm{Add}_\rho(\vec{q}^0, \vec{q}^1, \vec{q}^2) \wedge \mathrm{Add}_\rho(\vec{r}^0, \vec{r}^1, \vec{r}^2) \rightarrow \mathrm{Less}_\rho(\vec{q}^0, \vec{r}^0)$.

Furthermore, the Frege proof of (a) *has size $O(\rho^5)$, and the Frege proofs of* (b) *and* (c) *have size $O(\rho^8)$.*

The import of Lemma 2 is that propositional versions of ordinary facts regarding addition and equality and inequality have short proofs of polynomial size.

PROOF. We shall outline a description of the Frege proof for (c) and leave the rest to the reader. The Frege proof splits into two cases depending on whether $\mathrm{EQ}_\rho(\vec{q}^{\,1},\vec{r}^{\,1})$ or $\mathrm{Less}(\vec{q}^{\,1},\vec{r}^{\,1})$. Let us consider only the case of equality. By $\mathrm{Less}_\rho(\vec{q}^{\,2},\vec{r}^{\,2})$ we have that there is some k such that

$$\neg q_k^2 \wedge r_k^2 \wedge \bigwedge_{k<j\le\rho} (q_j^2 \leftrightarrow r_j^2).$$

Since $\neg r_\rho^2$, we have $0 \le k < \rho$ and the Frege proof further splits into ρ cases depending on the value of k. Let $\mathrm{Carry}_i(\vec{x},\vec{y})$ be the formula

$$\bigvee_{0\le j<i}\left(x_j \wedge y_j \wedge \bigwedge_{j<e<i}(x_e \oplus y_e)\right)$$

which expresses that there is a "carry" into the 2^i-column when adding $\vec{x}$ and $\vec{y}$. (Compare to the definition of Add_ρ.) The Frege proof now splits into 4 cases depending on the truth values of $\mathrm{Carry}_k(\vec{q}_1,\vec{q}_2)$ and $\mathrm{Carry}_k(\vec{r}_1,\vec{r}_2)$. The first three cases are when $\mathrm{Carry}_k(\vec{q}_1,\vec{q}_2) \to \mathrm{Carry}_k(\vec{r}_1,\vec{r}_2)$ and in each of these it is not too hard to prove

$$\bigvee_{m\ge k}\left(\neg q_m^0 \wedge r_m^0 \wedge \bigwedge_{m<j\le\rho}(q_j^0 \leftrightarrow r_j^0)\right)$$

with a Frege proof with $O(\rho^3)$ lines, so $\mathrm{Less}_\rho(\vec{q}^{\,0},\vec{r}^{\,0})$ holds. The fourth case is when $\mathrm{Carry}_k(\vec{q}_1,\vec{q}_2) \wedge \neg\mathrm{Carry}_k(\vec{r}_1,\vec{r}_2)$. In this case there is a Frege proof of $\bigwedge_{k\le j\le\rho}(q_j^0 \leftrightarrow r_j^0)$ with $O(\rho^3)$ lines. We then prove for $m = k, k-1,\ldots,0$ that

$$\bigvee_{m\le n<k}\left(r_n^0 \wedge \neg q_n^0 \wedge \bigwedge_{n<j\le\rho}(q_j^0 \leftrightarrow r_j^0)\right)$$
$$\vee\left(\bigwedge_{m\le j\le\rho}(q_j^0 \leftrightarrow r_j^0) \wedge \mathrm{Carry}_m(\vec{q}^{\,1},\vec{q}^{\,2}) \wedge \neg\mathrm{Carry}_m(\vec{r}^{\,1},\vec{r}^{\,2})\right)$$

by a straightforward Frege proof with $O(\rho^4)$ lines. But, of course, $\neg\mathrm{Carry}_0(\vec{q}^{\,1},\vec{q}^{\,2})$, so

$$\bigvee_{0\le n\le\rho}\left(r_n^0 \wedge \neg q_n^0 \wedge \bigwedge_{n<j\le\rho}(q_j^0 \leftrightarrow r_j^0)\right),$$

i.e., $\mathrm{Less}_\rho(\vec{q}^{\,0},\vec{r}^{\,0})$.

This completes the outline of the Frege proof of (c). Careful inspection of the proof shows it has $O(\rho^5)$ lines and every formula in the proof has size $O(\rho^3)$; hence the total size of the proof is $O(\rho^8)$. Q.E.D. Lemma 2.

Unfortunately, the above treatment of addition is not efficient enough for our purposes and instead we must use a technique called "carry-save-addition". Carry-save-addition is a well-known technique for computing the summation of a vector of numbers with a logarithmic depth circuit (see Savage [6]). As we see below, it allows us to define counting with polynomial size propositional formulae; without the use of carry-save addition formulae of size $O(n^{\log(\log n)})$ would be required.

DEFINITION. Let $\rho \geq 0$ and let $\varphi_0^l, \ldots, \varphi_\rho^l$ $(0 \leq l \leq 4)$ be proportional formulae. We define $\mathrm{CSum}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2, \vec{\varphi}^3, \vec{\varphi}^4)$ to be the conjunction of the following formulae:

$$\varphi_i^0 \leftrightarrow \varphi_i^2 \oplus \varphi_i^3 \oplus \varphi_i^4 \qquad (0 \leq i \leq \rho),$$

$$\varphi_0^1 \leftrightarrow p_0 \wedge \neg p_0,$$

$$\varphi_i^1 \leftrightarrow (\varphi_{i-1}^2 \wedge \varphi_{i-1}^3) \vee (\varphi_{i-1}^2 \wedge \varphi_{i-1}^4) \vee (\varphi_{i-1}^3 \wedge \varphi_{i-1}^4) \qquad (1 \leq i \leq \rho).$$

The point of defining carry-save addition is that we can combine 3 numbers, say n_2, n_3, n_4, to produce numbers n_0, n_1 such that the sum $n_2 + n_3 + n_4$ is equal to $n_0 + n_1$. The number n_0 is the bitwise sum modulo 2 of n_2, n_3 and n_4, and n_1 is the carries which are saved. It will be convenient for us to use carry-save addition to combine four numbers into two with the following definition.

DEFINITION. Let $\rho \geq 0$, and let $\varphi_0^l, \ldots, \varphi_\rho^l$ be propositional formulae for $0 \leq l \leq 5$. Then $\mathrm{CSAdd}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2, \vec{\varphi}^3, \vec{\varphi}^4, \vec{\varphi}^5)$ is the formula $\mathrm{CSum}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\psi}^0, \vec{\psi}^1, \vec{\varphi}^5)$ where $\vec{\psi}^0$ and $\vec{\psi}^1$ are the propositional formulae defined by

$$\psi_i^0 \equiv \varphi_i^2 \oplus \varphi_i^3 \oplus \varphi_i^4 \qquad (0 \leq i \leq \rho),$$

$$\psi_0^1 \equiv p_0 \wedge \neg p_0,$$

$$\psi_i^1 \equiv (\psi_{i-1}^2 \wedge \varphi_{i-1}^3) \vee (\varphi_{i-1}^2 \wedge \varphi_{i-1}^4) \vee (\varphi_{i-1}^3 \wedge \varphi_{i-1}^4) \qquad (1 \leq i \leq \rho).$$

The reason carry-save addition, CSAdd, is useful is that Lemma 1 can be improved upon:

LEMMA 3. *Suppose $\varphi_0^l, \ldots, \varphi_\rho^l$ for $2 \leq l \leq 5$, are propositional formulae. Let $\varphi_0^r, \ldots, \varphi_\rho^r$ for $r = 0, 1$ be the natural propositional formulae such that $\mathrm{CSAdd}_\rho(\vec{\varphi}^0, \vec{\varphi}^1, \vec{\varphi}^2, \vec{\varphi}^3, \vec{\varphi}^4, \vec{\varphi}^5)$ is true by definition, and let m be the maximum of the sizes of the φ_i^l's for $2 \leq l \leq 5$. Then the size of each φ_i^0 and φ_i^1 is less than $c \cdot m$, where c is a constant* (*independent of ρ and m*).

The proof of Lemma 3 is trivial; the next lemma states that polynomial-sized Frege proofs can show that carry-save-addition is equivalent to addition.

LEMMA 4. *There is a constant $k \geq 0$ such that for all $\rho \geq 0$ there is a Frege proof of size $O(\rho^k)$ of*

$$\begin{aligned} &\mathrm{CSAdd}_\rho(\vec{q}^0, \vec{q}^1, \vec{q}^2, \vec{q}^3, \vec{q}^4, \vec{q}^5) \wedge \mathrm{Add}_\rho(\vec{q}^6, \vec{q}^0, \vec{q}^1) \\ &\quad \wedge \mathrm{Add}_\rho(\vec{q}^7, \vec{q}^2, \vec{q}^3) \wedge \mathrm{Add}_\rho(\vec{q}^8, \vec{q}^4, \vec{q}^5) \wedge \mathrm{Add}_\rho(\vec{q}^9, \vec{q}^7, \vec{q}^8) \rightarrow \mathrm{EQ}_\rho(\vec{q}^6, \vec{q}^8). \end{aligned}$$

A direct proof of Lemma 4 is relatively straightforward, and we leave the details to the reader. Actually $k = 6$ suffices.

The next definition will give an efficient means for defining and reasoning about counting. It is assumed, without loss of generality, that n is equal to $2^{\rho-1}$ for some $\rho \geq 1$. If $\varphi_0, \ldots, \varphi_{n-1}$ are formulae, we want to be able to define the notion of the cardinality of the set $\{i \colon \varphi_i\}$, i.e., to count how many φ_i's are true.

DEFINITION. Let $\rho \geq 1$ and $n = 2^{\rho-1}$, and suppose $s_0^{i,j}, \ldots, s_\rho^{i,j}, c_0^{i,j}, \ldots, c_\rho^{i,j}$ are propositional formulae for $0 \leq i < \rho$ and $0 \leq j < n \cdot 2^{-i}$. The formula $\mathrm{VSum}_{\rho,k}(\vec{s}, \vec{c})$, where $1 \leq k < \rho$, is defined to be

$$\bigwedge_{i=1}^{k} \bigwedge_{j=0}^{n \cdot 2^{-i}-1} \mathrm{CSAdd}_\rho(\vec{s}^{i,j}, \vec{c}^{i,j}, \vec{s}^{i-1,2j}, \vec{c}^{i-1,2j}, \vec{s}^{i-1,2j+1}, \vec{c}^{i-1,2j+1})$$

and $\mathrm{VSum}_\rho(\vec{s}, \vec{c})$ is defined to be $\mathrm{VSum}_{\rho,\rho-1}(\vec{s}, \vec{c})$.

Suppose that each φ_i, $c_k^{i,j}$ and $s_k^{i,j}$ have been assigned truth values so that $\varphi_i \leftrightarrow s_0^{0,i}$ for $0 \le i < n$, each $s_{k+1}^{0,i}$ and each $c_k^{0,i}$ are assigned "false" and that $\mathrm{VSum}_\rho(\vec{s}, \vec{c})$ is valid. Let $S^{i,j}$ be the number represented by $\vec{s}^{\,i,j}$ and $C^{i,j}$ the number represented by $\vec{c}^{\,i,j}$. Then it is easy to see by induction on i that $C^{i,j} + S^{i,j}$ is equal to the number of true φ_k's with $2^i \cdot j \le k < 2^i(j+1)$. In particular, $C^{\rho-1,0} + S^{\rho-1,0}$ is equal to the total number of φ_k's which are true. Accordingly, we make the following definition for counting:

DEFINITION. Let $\rho \ge 1$ and $n = 2^{\rho-1}$; let $\varphi_0, \ldots, \varphi_{n-1}$ be propositional formulae and suppose $s_k^{i,j}$, $c_k^{i,j}$, $a_k^{i,j}$ are propositional formulae for $0 \le i < \rho$, $0 \le j < n \cdot 2^{-i}$ and $0 \le k \le \rho$. The formula $\mathrm{Count}_{\rho,r}(\vec{a}, \vec{s}, \vec{c}, \vec{\varphi})$ is defined to be the conjunction of the following formulae:

$$\mathrm{VSum}_{\rho,r}(\vec{s}, \vec{c}),$$

$$\bigwedge_{i=0}^{r} \bigwedge_{j=0}^{n\cdot 2^{-i}-1} \mathrm{Add}_\rho(\vec{a}^{\,i,j}, \vec{s}^{\,i,j}, \vec{c}^{\,i,j}),$$

$$\bigwedge_{j=0}^{n-1} \left((\vec{s}_0^{\,0,j} \leftrightarrow \varphi_j) \wedge \bigwedge_{k=1}^{\rho} \neg \vec{s}_k^{\,0,j} \wedge \bigwedge_{k=0}^{\rho} \neg \vec{c}_k^{\,0,j} \right);$$

and $\mathrm{Count}_\rho(\vec{a}, \vec{s}, \vec{c}, \vec{\varphi})$ is just $\mathrm{Count}_{\rho,\rho-1}(\vec{a}, \vec{s}, \vec{c}, \vec{\varphi})$.

LEMMA 5. *Let $\rho \ge 1$ and $n = 2^{\rho-1}$.*

(a) *Suppose each $s_k^{0,j}$ and $c_k^{0,j}$ is a propositional formula of size $\le m$ for $0 \le j < n$ and $0 \le k \le \rho$. Define $s_k^{i,j}$ and $c_k^{i,j}$ for $1 \le i < \rho$, $0 \le j < 2^{-i} \cdot n$, $0 \le k \le \rho$ to be the natural formulae for which* $\mathrm{VSum}_\rho(\vec{s}, \vec{c})$ *holds. Then there is a constant c, independent of m and n, such that the size of each $s_k^{i,j}$ and $c_k^{i,j}$ is less than $m \cdot n^c$.*

(b) *Suppose each $\varphi_0, \ldots, \varphi_{n-1}$ is a propositional formula of size $\le m$. Define $s_k^{i,j}$ and $c_k^{i,j}$ and $a_k^{i,j}$ for $0 \le i < \rho$, $0 \le j < 2^{-i} \cdot n$, $0 \le k \le \rho$ to be the natural formulae for which* $\mathrm{Count}_\rho(\vec{a}, \vec{s}, \vec{c}, \vec{\varphi})$ *holds. Then there is a constant c', independent of m and n, such that the size of each $a_k^{i,j}$, $s_k^{i,j}$ and $c_k^{i,j}$ is less than $c' \cdot m \cdot n^{c'}$.*

PROOF. Let d be the constant guaranteed to exist by Lemma 3. By iteratively applying Lemma 3, it follows that each $s_k^{i,j}$ and $c_k^{i,j}$ has size $\le d^i \cdot m$, i.e., they have size $\le d^{(\log_2 n)} \cdot m$. Picking $c = \log_2 d$ makes (a) hold.

Let b be the constant guaranteed to exist by Lemma 1. Then each $a_k^{i,j}$ has size $\le b \cdot \rho^3 \cdot n^c \cdot m$. Since $\rho = 1 + \log_2 n$, we may choose c' slightly larger than b and c and have (b) hold. Q.E.D. Lemma 5.

LEMMA 6. *There is a constant $k \ge 0$ such that for all $n = 2^{\rho-1}$ there are Frege proofs of size $O(n^k)$ of*

$$\bigwedge_{j=0}^{n-1} (r_j \wedge \neg r'_j) \wedge \mathrm{Count}_\rho(\vec{a}, \vec{s}, \vec{c}, \vec{r}) \wedge \mathrm{Count}_\rho(\vec{b}, \vec{t}, \vec{d}, \vec{r}\,') \to \mathrm{LE}_\rho(\vec{a}^{\,\rho-1,0}, \vec{b}^{\,\rho-1,0})$$

and of

$$\bigvee_{j=0}^{n-1} (r_j \wedge \neg r'_j) \wedge \bigwedge_{j=0}^{n-1} (r'_j \to r_j) \wedge \mathrm{Count}_\rho(\vec{a}, \vec{s}, \vec{c}, \vec{r}) \wedge \mathrm{Count}_\rho(\vec{b}, \vec{t}, \vec{d}, \vec{r}\,')$$
$$\to \mathrm{Less}_\rho(\vec{a}^{\,\rho-1,0}, \vec{b}^{\,\rho-1,0}).$$

PROOF. Let A_ρ be the propositional formula

$$\bigwedge_{j=0}^{n-1} (r'_j \to r_j) \wedge \mathrm{Count}_\rho(\vec{a}, \vec{s}, \vec{c}, \vec{r}) \wedge \mathrm{Count}_\rho(\vec{b}, \vec{t}, \vec{d}, \vec{r}\,').$$

The Frege proof of the first formula proceeds by showing the intermediate results

$$A_\rho \to \mathrm{LE}_\rho(\vec{a}^{\,i,j}, \vec{b}^{\,i,j}) \wedge \mathrm{LE}_\rho(\vec{b}^{\,i,j}, \overline{2^i}),$$

for $i = 1, \ldots, \rho - 1$ and $0 \le j < n \cdot 2^{-i}$. These are proved by using the proofs described by Lemmas 2 and 4. There are only $O(n^2)$ such intermediate steps, so it is clear that this gives a polynomial size proof of

$$A_\rho \to \mathrm{LE}_\rho(\vec{a}^{\,\rho-1,0}, \vec{b}^{\,\rho-1,0}).$$

For m any integer, $0 \le m < n$, let $B_{m,\rho}$ be the formula $r_m \wedge \neg r'_m \wedge A_\rho$. In addition to the consequences of A_ρ derived above, we also prove that for all $i = 0, \ldots, \rho - 1$ and j such that $j \cdot 2^i \le m < (j+1) \cdot 2^i$

$$B_{m,\rho} \to \mathrm{Less}_\rho(\vec{a}^{\,i,j}, \vec{b}^{\,i,j});$$

again, this is proved using Lemmas 2 and 4. The n proofs for all values of m can be combined to give the desired proof of

$$\bigvee_{j=0}^{n-1} (r_j \wedge r'_j) \wedge A_\rho \to \mathrm{Less}_\rho(\vec{a}^{\,\rho-1,0}, \vec{b}^{\,\rho-1,0}). \quad \text{Q.E.D. Lemma 6.}$$

We are now ready to prove that there are polynomial size Frege proofs of the propositional pigeonhole principle.

MAIN THEOREM 7. *There is a constant k such that there are Frege proofs of size $O(n^k)$ of* PHP_n.

PROOF. Recall that PHP_n is

$$\bigwedge_{0 \le i \le n} \bigvee_{0 \le j < n} p_{i,j} \to \bigvee_{0 \le i < m \le n} \bigvee_{0 \le j < n} (p_{i,j} \wedge p_{m,j}).$$

Assume without loss of generality that n is a power of two and $n = 2^{\rho-1}$. For conceptual convenience we will describe a polynomial size extended Frege (e$\mathscr{F}$) proof of PHP_n and afterwards analyze the size of the Frege proof obtained by replacing propositional variables introduced by the extension rule with the formulae they abbreviate. First, we introduce new propositional variables r_j^m for $0 \le m \le n$ and $0 \le j < n$ defined by $r_j^m \leftrightarrow \bigvee_{0 \le k \le m} p_{k,j}$. Second, we introduce variables $a_k^{m,i,j}$, $s_k^{m,i,j}$, $c_k^{m,i,j}$ for all $0 \le m \le n$ and all appropriate values of i, j and k so that, for all m, $\mathrm{Count}_\rho(\vec{a}^{\,m}, \vec{s}^{\,m}, \vec{c}^{\,m}, \vec{r}^{\,m})$ holds. If we think of the variables $p_{i,j}$ representing the graph of a function mapping pigeons to holes, then $\vec{a}^{\,m,\rho-1,0}$ represents the number of holes j mapped onto by the first $m+1$ pigeons.

There is a simple proof that $\neg\mathrm{PHP}_n \to \bigvee_{0 \le j < n} r_j^0$. Hence, by Lemma 6, there is a polynomial size proof of

$$\neg\mathrm{PHP}_n \to \mathrm{Less}_\rho(\bar{0}, \vec{a}^{\,0,\rho-1,0}).$$

Similarly, by Lemma 6, there are n polynomial size proofs of

$$\neg\mathrm{PHP}_n \to \mathrm{Less}_\rho(\vec{a}^{\,m,\rho-1,0}, \vec{a}^{\,m+1,\rho-1,0})$$

for $m = 0, 1, \ldots, n-1$. Now it is not difficult to combine these proofs to get polynomial size proofs of

$$\neg\mathrm{PHP}_n \to \mathrm{Less}_\rho(\bar{m}, \vec{a}^{\,m,\rho-1,0}).$$

In particular,

$$\neg \mathrm{PHP}_n \rightarrow \mathrm{Less}_\rho(\bar{n}, \vec{a}^{n,\rho-1,0}).$$

But it is straightforward to prove, using the kind of reasoning used in the proof of Lemma 6, that $\mathrm{LE}_\rho(\vec{a}^{n,\rho-1,0}, \bar{n})$. Thus,

$$\neg \mathrm{PHP}_n \rightarrow \mathrm{Less}_\rho(\bar{n}, \bar{n})$$

and clearly $\neg \mathrm{Less}_\rho(\bar{n}, \bar{n})$, so PHP_n. This completes the description of the polynomial size extended Frege proof of PHP_n.

It is easy to verify that this proof of PHP_n has its number of lines bounded by a polynomial of n. Furthermore, Lemma 5(b) shows that if the propositional variables introduced by the extension rule are replaced by the formulae they abbreviate, then polynomial sized Frege proofs of PHP_n are obtained. Q.E.D. Main Theorem.

Although we have not analyzed the Frege proofs of PHP_n carefully enough to determine the degree of the polynomial bounding the size of the Frege proofs, it is clear that the degree is fairly small, e.g., there are Frege proofs of PHP_n of size $O(n^{20})$.

§5. Connections to provability in bounded arithmetic. This section briefly discusses some connections between the existence of short Frege proofs of the propositional pigeonhole principle and of proofs of a relativized pigeonhole principle in the first order theories of bounded arithmetic. The situation described below is somewhat analogous to the relationship between constant depth, polynomial size circuits and the relativized polynomial hierarchy as discussed by Furst-Saxe-Sipser [3], Yao [12] and others.

DEFINITION. The Σ_k- and Π_k-formulae are defined inductively as follows:

(1) A propositional variable is a Σ_0-formula and a Π_0-formula.

(2) If A is a Σ_i-formula (Π_i-formula) then $\neg A$ is a Π_i-formula (Σ_i-formula).

(3) If $A_1, \ldots, A_n$ are Σ_i-formulae (Π_i-formulae) then any conjunction (disjunction) of them is a Π_{i+1}-formula (Σ_{i+1}-formula).

(4) If A_1 is a Σ_i-formula and A_2 is a Π_i-formula then $A_1 \rightarrow A_2$ is a Σ_{i+1}-formula and $A_2 \rightarrow A_1$ is a Σ_i-formula.

We say that the propositional pigeonhole principle has *constant formula-depth, polynomial size* Frege proofs iff there is a constant k such that for all n there is a Frege proof of PHP_n of size $\leq n^k + k$ in which each formula is a Σ_k-formula. The next proposition is due to Paris and Wilkie and is a slight strengthening of Theorem 26 of [5]. It is proved by the same proof as in [5], or alternatively, a constructive proof may be given by combining Paris and Wilkie's ideas with a strengthening of Theorem 4.10 of [1].

DEFINITION. Let $I\Delta_0(f)$ be $I\Delta_0$ with a new unary function symbol f which may be used in induction formulae. Let $\mathrm{PHP}(f)$ be the sentence

$$(\forall x)[(\forall y \leq x)(f(y) < x) \rightarrow (\exists y)(\exists z)(y \neq z \wedge f(y) = f(z))].$$

PROPOSITION 8 (PARIS AND WILKIE [5]). *If $I\Delta_0(f) \vdash \mathrm{PHP}(f)$ then there are constant formula-depth, polynomial size Frege proofs of the propositional pigeonhole principle.*

The next theorem states that if there is an additional uniformity condition on the Frege proofs of PHP_n then the converse of Proposition 8 holds.

THEOREM 9. *Suppose $I\Delta_0$ can define constant formula-depth, polynomial size Frege proofs of* PHP_n; *more precisely, suppose there is a Δ_0-function $G(n,x)$ of $I\Delta_0$ such that the graph of $G(n,-)$ codes a constant formula-depth, polynomial size Frege proof of* PHP_n *provably in $I\Delta_0$. Then $I\Delta_0(f)\vdash \mathrm{PHP}(f)$.*

Also the same result holds for $I\Delta_0+\Omega_1$ if "polynomial size" is replaced by "size $O(2^{(\log n)^k})$ for fixed k independent of n".

PROOF (SKETCH). Let $G(n,-)$ be as in the hypothesis. Working in $I\Delta_0(f)$, let n be an arbitrary integer. A truth predicate T_k can be defined for Σ_k-formulae by interpreting $p_{i,j}$ to be true iff $f(i)=j$. Furthermore, T_k is defined by a bounded formula and provably satisfies the usual inductive properties of a truth predicate. Now it can be shown that each axiom of the proof coded by $G(n,-)$ is true and each inference in $G(n,-)$ preserves truth. Since G is defined by a bounded formula, it follows by bounded induction that the final line of the proof is true, i.e., that $\mathrm{PHP}(f)$ is true. Q.E.D. Theorem 9.

The hypothesis of Theorem 9 is a very reasonable assumption to put on constant formula depth, polynomial size Frege proofs; at least if the proofs are uniform enough to be definable in the log-time hierarchy. Most reasonable constructions of constant formula-depth, polynomial size proofs would make the hypothesis of Theorem 9 true. It follows that we should expect the relativized pigeonhole principle to be provable in bounded arithmetic iff there are constant formula depth, polynomial size Frege proofs of the propositional pigeonhole principle.

It seems probable that there are no constant formula depth, polynomial size Frege proofs of the propositional pigeonhole principle, and hence $\mathrm{PHP}(f)$ is not a theorem of $I\Delta_0$. Some partial results are known: the proof of Theorem 5.13 of [1] shows $S_2^1(f)$ does not prove $\mathrm{PHP}(f)$ and, similarly, Theorem 21 of Paris and Wilkie [5] shows that $I\exists_1(f)$ does not prove $\mathrm{PHP}(f)$.

Haken [4] has shown that for some constant c, every resolution proof of PHP_n has size at least c^n. Combining this with the Main Theorem 7 above shows that Frege proof systems have an exponential speedup over resolution, a fact which was originally proved by A. Urquhart.

THEOREM 10. *The propositional pigeonhole principle is a family of formulae* PHP_n *which have polynomial size Frege proofs but require exponential size resolution proofs.*

It would be interesting to know whether depth k Frege proofs can p-simulate depth $k+1$ Frege proofs, e.g., does there exist a family of Σ_k-formulae which have constant formula depth, polynomial size Frege proofs but do not have polynomial size Frege proofs using only Σ_k-formulae?

Acknowledgements. I have benefited from discussions with A. Wilkie and especially P. Shor, who suggested the use of carry-save addition.

REFERENCES

[1] S. BUSS, ***Bounded arithmetic***, Ph.D. Thesis, Princeton University, Princeton, New Jersey, 1985.

[2] S. COOK and R. RECKHOW, *The relative efficiency of propositional proof systems*, this JOURNAL, vol. 44 (1979), pp. 36–50.

[3] M. FURST, J. SAXE and M. SIPSER, *Parity, circuits and the polynomial-time hierarchy*, ***IEEE Symposium on Foundation of Computing***, vol. 22 (1981), pp. 260–270.

[4] A. HAKEN, *The intractability of resolution*, ***Theoretical Computer Science***, vol. 39 (1985), pp. 297–308.

[5] J. PARIS and A. WILKIE, *Counting problems in bounded arithmetic*, ***Methods in Mathematical Logic (Proceedings, Caracas, 1983)***, Lecture Notes in Mathematics, vol. 1130, Springer-Verlag, Berlin, 1985, pp. 317–340.

[6] J. E. SAVAGE, ***The complexity of computing***, Wiley, New York, 1976.

[7] R. STATMAN, *Complexity of derivations from quantifier-free Horn formulae, mechanical introduction of explicit definitions, and refinement of completeness theorems*, ***Logic Colloquium '76*** (R. Gandy and M. Hyland, editors), North-Holland, Amsterdam, 1977, pp. 505–517.

[8] G. S. TSEĬTIN, *On the complexity of derivation in propositional calculus*, ***Studies in constructive mathematics and mathematical logic. II*** (A. O. Slisenko, editor), ***Zapiski Nauchnykh Seminarov LOMI***, vol. 8 (1968), pp. 234–259; English translation, ***Seminars in Mathematics, V. A. Steklov Mathematical Institute, Leningrad***, vol. 8, Consultants Bureau, New York, 1970, pp. 115–125.

[9] A. WILKIE, Talk presented at Logic Colloquium '84, Manchester, 1984.

[10] A. WOODS, ***Some problems in logic and number theory and their connections***, Ph.D. Thesis, Manchester University, Manchester, 1981.

[11] A. URQUHART, *Hard examples for resolution*, ***Journal of the Association for Computing Machinery***, vol. 34 (1987), pp. 209–219.

[12] A. YAO, *Separating the polynomial-time hierarchy by oracles*, ***IEEE Symposium on Foundations of Computing***, vol. 26 (1985), pp. 1–10.

MATHEMATICAL SCIENCES RESEARCH INSTITUTE
BERKELEY, CALIFORNIA 94720

Current address: Department of Mathematics, University of California, Berkeley, California 94720.