The Surjective Weak Pigeonhole Principle in Bounded Arithmetic

Chris Pollett
San Jose State University

Feb. 1, 2008.

What this talk is about…

We intend to give a survey of:

- Bounded Arithmetic
- In particular, the role of the Pigeonhole Principle in these weak systems of arithmetic
- And how the surjective pigeonhole principle plays a role in the reverse mathematics of Komolgorov Complexity results in these systems.

Bounded Arithmetics

- Have BASIC axioms like:

  $y \leq x \supset y \leq S(x)$

  $x+Sy = S(x+y)$

  for the symbols $0, S, +, \cdot, x\#y := 2^{|x||y|}, |x| :=$ length of x, $\dot{-}$, $\lfloor x/2^i \rfloor$, $\leq$
- Have IND_m induction axioms of the form:

  $A(0) \wedge \forall x<|t|_m[A(x) \supset A(S(x))] \supset A(|t|_m)$

  Here t is a term made of compositions of variables and our function symbols and $|x|_0=x$, $|x|_m=| |x|_{m-1}|$.
- Have a language with:
  - Limited subtraction ($\dot{-}$) and $\lfloor x/2^i \rfloor$ which allows one to project out blocks of bits and do sequence coding using just terms in the language.
  - Smash (#) which allows the length of terms to grow polynomially in the length of the inputs, which is useful for defining complexity classes like NP.

Bounded Arithmetics cont'd

- A $\sum^b_i$**-formula** is a formula of the form:

  $\exists x_1 \leq t_1 \forall x_2 \leq t_2 \cdots Qx_i \leq t_i\ Qx_{i+1} \leq |t_{i+1}| A$

  i+1 alternations, innermost begin length bounded

where A is an open formula. A $\prod^b_i$-formula is defined similarly but with the outer quantifier being universal.

- By a **bounded formula** we will mean a formula all of whose quantifiers are bounded.
- **Fact:** $\sum^b_1$-sets are precisely the NP-sets (nondeterministic polynomial time sets); $\prod^b_1$-sets are the co-NP sets, etc.
- Let

  T^i_2 is the theory BASIC + $\sum^b_i$-IND_0

  S^i_2 is the theory BASIC + $\sum^b_i$-IND_1

  R^i_2 is the theory BASIC + $\sum^b_i$-IND_2

- If we add to the language a function symbol $x\#_3y$ with $|x\#_3y|=|x|\#|y|$, then get theories T^i_3, S^i_3, R^i_3.

Well-known Results

Parikh's Theorem. Let A be a bounded formula. If one of our bounded arithmetic theories T proves $\forall x \exists y A(x,y)$ then there is a term t such that T proves $\forall x \exists y \leq t A(x,y)$.

- This has both a proof theory based proof and a compactness argument proof. It shows that functions of exponential growth are not definable in bounded arithmetic.

Buss' Theorem. The Σ^b_1-definable functions of S^1_2 are precisely the polynomial time computable functions, the class FP.

Conservativity. (Buss)(Jerabek i = 0) For $i \geq 0$, S^{i+1}_2 is Σ^b_{i+1} conservative over T^i_2.

Pigeonhole Principles

Let $m > n$. Given a relation $R(x,y,z)$

- $iPHP^m_n(R)$:

  $\forall x < m \, \exists! \, y < n \; R(x,y,z) \supset$

  $\exists x_1,x_2 < m \, \exists y < n \, [x_1 \neq x_2 \wedge R(x_1,y,z) \wedge R(x_2,y,z)]$

  If R is a function from *m* into *n*, it is not one-to-one (two points map to the same value).

- $sPHP^m_n(R)$:

  $\forall x < n \, \exists! \, y < m \; R(x,y,z) \supset \exists y < m \forall x < n \neg R(x,y,z)$

  If R is a function from *n* into *m*, then it is not onto (some value for y is missed).

- $mPHP^m_n(R)$:

  $\forall x < m \, \exists y < n \; R(x,y,z) \supset$

  $\exists x_1,x_2 < m \, \exists y < n \, [x_1 \neq x_2 \wedge R(x_1,y,z) \wedge R(x_2,y,z)]$

  If R is a multifunction from *m* into *n* it is not one-to-one (two points map to the same value).

These principles for a class of relations C is denoted by $vPHP^m_n(C)$ where v=i,s, or m. We will write PV for p-time relations.

How much power does the weak pigeonhole principle add?

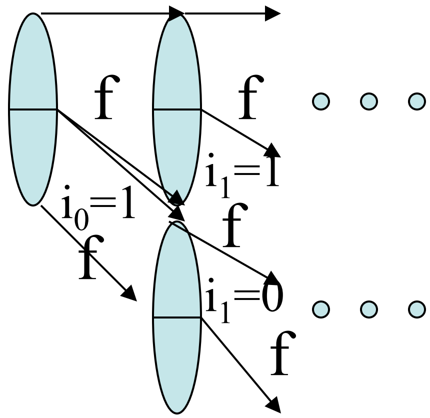
- By a weak pigeonhole principle we will mean the case where $m \geq 2n$. The main reason for interest in these cases rather than using $m = n+1$ is that the string length changes.
- BASIC(R) proves $mPHP^m_n(R)$ implies both $sPHP^m_n(R)$ and $iPHP^m_n(R)$.
- $S^1_2(R)$ proves $mPHP^n_{|n|}(R)$.
- (Maciel, et al) $T^2_2(R)$ proves $mPHP^{n^2}_n(R)$.
- (Wilkie) The Σ^b_1-definable functions of $S^1_2(PV) + mPHP^{n^2}_n(PV)$ can be witnessed by multifunctions from RP, randomized p-time.
- (Jerabek) If $S^1_2 + sPHP^{n^2}_n(PV)$ proves $iPHP^{n^2}_n(PV)$ then factoring is in probabilistic p-time.

Surjective Weak Pigeonhole Principle and Hard Strings

- Let n=|x|, the length of our input sizes. Let $HARD_k$ be the formalization of the statement: “There is a string S of length at most $2n^k$ whose bit values are not the output of any circuit of size n^k on inputs $0^{|x|}, 0^{|x|}+1,.., 0^{|x|} + 2n^k-1$.”
- It is straightforward to define a function from circuits of size n^k to strings of length at most $2n^k$. Applying $sPHP^{x^2}_x(PV)$ to this implies $HARD_k$ over S^1_2.
- It turns out (Jerabek ’04) has shown over S^1_2 that $sPHP^{x^2}_x(PV)$ and the $HARD_k$ principles are equivalent
- For $HARD_k \supset sWPHP(PV)$, suppose there is a p-time function f for which the sWPHP fails…
- Then there is a $n^{k'}$ size circuit family $\{C^f_n\}$ computing this function for some k'. Can iterate f according to a string $i_0 i_1 \cdot\cdot$

More Hard Strings

Input: 2n bit string. $(2^{|x|})^2 = 2^{2|x|}$, n=|x|



For any k>k' , iterating C^f_n O(|n|) times, we can get a circuit C' of size $n^{k'+1}$ whose domain is $|2n^{k-1}|$ x 2n-bit numbers but whose range is all strings of size $2n^k$.

Let C be the circuit which on input i $<2n^k$ and s and an 2n bit number computes the ith bit of C'. For any fixed S of length $<2n^k$ we can now hard code the s that maps to it in C to get a circuit showing S is not the hard string of $HARD_k$.

In a similar fashion (Pollett-Danner'05) have come up with an iterated hard block principle that is equivalent to $mPHP^{x\^2}_x(Iter(PV,\log^{O(1)}))$ over S^1_2.

Komolgorov Complexity Arguments in Bounded Arithmetic

- Many textbook examples (Li Vitanyi) of proofs using Komolgorov complexity, to show computational complexity results, number theory results, or combinatorics rely on the existence of a hard string of the kind we just discussed.
- This suggests trying to formalize them in of S^1_2 together with the surjective weak pigeonhole principle for some complexity class.
- We now consider a couple of examples where this was taken as the starting point and then modifications were done to get proofs that work.

Complexity Theory

(Danner-Pollett) $S^1_2 + psPHP^{n\char`^2}_n(\Sigma^b_1)$ proves that recognizing the language $\{x0^{|x|}x \mid x \text{ in } \{0,1\}^*\}$ on a 1-tape Turing machine (palindrome checking) in requires time $t(n) > \Omega(n^2)$. Here ps is for partial surjective.

The proof idea is to define a function cross_seq(e, x, w, i) which consists of the sequence of (state, tape square value) corresponding to the times where machine e on input x just before it did a move from square i to square i+1 in computation w. S^1_2 can prove that the sum of length of the crossing sequences $0 \leq i \leq |x|+t(|x|)$ is a lower bound on the length of the computation. Lemmas are then proven to show for m and i such that $m \leq i \leq 2m$ and crossing sequence c there is a unique x, $|x|=m$ and w such that cross_seq(e, $x0^{|x|}x$, w, i) =c. This gives a partial surjection from crossing sequences to strings. So at for some x the crossing sequence has $|x|$. As there are $|x|$ many i's, and the total runtime is greater than the sum of the crossing sequences this gives the result.

Number Theory

- Some older known results concerning weak pigeonhole principles are:
  - (Woods, Paris-Wilkie-Woods) S^1_2+iPHP$^{n^2}_n$(PV) proves for $1 \leq x < y$ one of y, y+1, …, y+x has a prime divisor $p > x$.
  - (Berarducci and Intraglia) $I\Delta_0$+WPHP(Δ_0) proves the four squares theorem. My suspicion is this proof can be pushed down to S^1_2+iPHP$^{n^2}_n$(PV). Proof establishes multiplicative properties of Legendre Symbol in the theory to show -1 is the sum of two squares mod p then uses recursive descent at most length many times.
- (Danner-Pollett) T^1_2+mPHP$^{n^2}_n$(PLS^{NP}) proves $\pi(x) \geq x/\log^2 x$. Here $\pi(x)$ is the number of primes $\leq$ x.

Some comments on the density of primes results

- If you have exponentiation you can define 2m choose m and carry out Chebyshev's lower bound of 1/2x/ln x.
- PWW result gives a lower bound around log x in S^1_2+i$PHP^{n\wedge 2}_n$(PV) .
- The idea is using PWW, you can argue the correctness of a PLS^{NP} local search algorithm for the *m*th prime. Here we can give a circuit to compute each step which has some fixed polynomial size, n^k, using some fixed oracle to get a next prime.
- Using T^1_2+s$PHP^{n\wedge 2}_n$(PLS^{NP}) can get a hard string result for such local searches.
- Given a number N you can uniquely encode it by m and $k=N/p_m$ where p_m is the *m*th prime. Choose the encoding as the code(|m|)mk. Here code($x_0\, x_1..x_n$)= $x_0 0\, x_1 0..\, x_n 1$. So this encoding has length 2log|m| +log m+ log(N/p_m)
- Using the hard string result, there is some N for which log N ≤ circuit size of local search problem to find N≤ 2log |m| + log m + log N - log p_m. This give $p_m \leq m \log^2 m$ from which the density result follows.

Combinatorics

- As a last couple of examples, I briefly mention some new results of Jerabek:
  - A **tournament** on n vertices is a directed graph such that for every i, j ≤ n exactly one of (i, j) and (j, i) is in the graph. A **dominating set** D in a tournament T is a set such for any j not in D there is an i in D with (i, j) in T. Tournaments play a role in proofs in complexity theory about selective sets. Let G be a new relation symbol. $S^2_2(G)$ + sWPHP($PV_2(G)$) proves a tournament on N vertices has a dominating set of size $|N|$.
  - A **clique** C in a graph is a set of vertices such that for every i, j in C the edge (i, j) is in C. $S^2_2(G)$ + sWPHP($PV_2(G)$) proves an undirected graph G on N vertices has either a clique or a co-clique of size 1/2log N.

Conclusion

- Hopefully, it seems plausible that some interesting reverse mathematics style results can be had in weak systems using weak pigeonhole principles.
- It would be interesting to know if any of these previous results is exact.
- For instance, can one show that palindrome checking is equivalent to

  $S^1_2 + psPHP^{n^2}_n(\Sigma^b_1)$?