When can S^1_2 prove the weak pigeonhole principle?

Chris Pollett

Apr. 10, 2006.

Outline

- Weak Pigeonhole Principles
- Function Algebras
- Binary Prefix Series (BPSs)
- BPS and our Algebras
- Hard Functions for our Algebras

Weak Pigeonhole Principles

- We will be interested in the m=n#n case of the following principles:
- $iPHP^m_n(f)$:

  $\forall n \forall \bar{z} [n<m \wedge \exists x < m\, f(x, \bar{z}) > n \vee \exists x_1, x_2 < m\, [x_1 \neq x_2 \wedge f(x_1, \bar{z}) = f(x_2, \bar{z})\,]$

  If f is a function from m >n into n, it is not one-to-one (two points map to the same value).
- $sPHP^m_n(f)$:

  $\forall n \forall \bar{z} [n<m \wedge \exists y < m\, \forall x < n\, f(x, \bar{z}) \neq y]$

  If *f* is a function from *n* into *m*>*n*, then it is not onto (some value for *y* is missed).
- When $m=n^2$, the above are called weak pigeonhole principles, denoted iWPHP(f) and sWPHP(f), respectively.
- In S^1_2 (:= BASIC + Σ^b_1-LIND) one can iterate f to prove the $m= n^2$ case implies the m=n#n case.
- That is, if v=i, s, then $vPHP^{n\#n}_n(f)$ trivially implies $vWPHP_n(f)$; whereas, we also have $vWPHP_n(\Sigma^b_1(f))$ implies $vPHP^{n\#n}_n(f)$.

More on Weak Pigeonhole Principles

- For what f can S^1_2 (:= BASIC + $\sum^b_1$-LIND) prove these pigeonhole principles?

  Krajíček and Pudlák showed that if S^1_2 could prove iWPHP(PV), that is for p-time functions, then RSA is insecure.

  Today's talk will be on for what f can we show $sPHP^{n\#n}_n(f)$ is provable in S^1_2.

  The argument probably works with parameters $\overline{z}$ but have only worked out the non-parameter case in detail.

Function Algebras

- One way to characterize *p*-time is to start off with some initial functions and close under composition and length bounded primitive recursion. We'll take our initial functions to be:

  Initial := variables, 0, S, +, –, $|x|$, PAD$(x, y) := x \cdot 2^{|y|}$, MSP$(x, y) = \lfloor x/ 2^{y} \rfloor$, $x\#y := 2^{|x||y|}$.

  – Notice there is no multiplication.

  – This is essentially the initial functions in some of Clote and Takeuti's papers for TAC^0.

  – It can define as a term pairing and a limited amount of sequence coding.

More Functions Algebras

- Our recursion scheme:

  f is defined from g, h, t and r by *m-length bounded primitive recursion* (m-BPR) if

  $$F(0, \bar{x}) = \mathrm{g}(\bar{x})$$

  $$F(n+1, \bar{x}) = \min(h(n, \bar{x}, F(n, \bar{x})), r(n, \bar{x}))$$

  $$f(n, \bar{x}) = F(|t(n, \bar{x})|_m, \bar{x})$$

  where $|x|_0 = x$, $|x|_{m+1} = ||x|_m|$ and r and t are terms over Initial.
- From this we define our algebras:

  A^m := closure of Initial under composition and m-BPR.
  - A^1 is the polynomial time functions.
  - We will argue that $sPHP^{n\#n}_n(A^3)$ is provable in S^1_2.

Our Approach

- Show in S^1_2 that if x is mapped by an A^3 function f:[N] --> [$N\#N$] then its image must be expressible by a certain kind of series.
- Show that in S^1_2 one can define a number HARD(N) which is hard for this kind of series for any $x < N$.
- This number will be our element not in the range of f.

Binary Prefix Series

- Our series are called Binary Prefix Series (BPS's) and can be defined with a predicate:

BPS(k, N, $\bar{x}$, S, t) :=

1. Each $x_m < N$,
2. S codes a sequence for the series

$$\sum_{i=1}^{k'} s_i 2^{j_i}$$

where $0 \leq k' \leq k$ and each $s_i = \pm\mathrm{MSP}(x_m, y)$, or $s_i = \pm 1$ for some y and some variable x_m

3. Evaluating S yields t.

- Given an f in A^3 our goal will be to put a bound on the k for which S^1_2 proves the condition

$$\forall \bar{x}\ \exists S\ \mathrm{BPS}(k(N), N, \bar{x}, S, f(x))$$

which we write as $C_f(N, k(N))$.

BPS's and our Algebras

- S^1_2 proves the following bounds on $C_f(N, k'(N))$ in terms of the complexities of the input argument k_1 , k_2 :
  - If f is 0, a variable x_m, or # then $k' = 1$
  - If f is S then $k' = k_1 + 1$.
  - If f is $|\cdot|$ then $k' = O(||N||)$
  - If f is PAD then $k' = k_1$
  - If f is MSP then $k' = 2k_1$
  - If f is +, – then can bound k' as $k_1 + k_2$.
- For composition, S^1_2 proves if f has complexity $k''(N)$ when all its arguments have complexity 1, then $f(\overline{u})$ will have complexity $k''(M)(2\sum k_i(N))$ when its arguments have complexity $k_i(N)$ and the max of their outputs has size M.
- From this the complexity of any Initial term is $||N||^{O(1)}$.
- Closing under m-BPR will give complexities

$$(||N||)^{(|N|_m)^{O(1)}}$$

Hard Functions for our Algebras

- Consider the Σ^b_1-defined in S^1_2 function

$$f(N) = \lfloor (2^{|N||N|} - 1)/3 \rfloor$$

- Given a BPS for some 1-input, A^3 function which supposedly maps [N] --> [N#N], S^1_2 can regroup the series to look like:

$$\mathrm{MSP}(x,0) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x,0))$$
$$\mathrm{MSP}(x,1) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x,1))$$
$$\ldots$$
$$\mathrm{MSP}(x, |N|) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x, |N|)$$

$$-\mathrm{MSP}(x,0) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x,0))$$
$$-\mathrm{MSP}(x,1) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x,1))$$
$$\ldots$$
$$-\mathrm{MSP}(x, |N|) \cdot (2^{k\_i} \text{ factor's for } \mathrm{MSP}(x, |N|)$$

- The $\mathrm{MSP}(x, i)$'s can further be viewed as $|N|$ bit numbers.
- S^1_2 can sum the jth bit of these numbers for rows which have a given 2^k value.
- This yields $|N|\cdot||N||^{(|||N|||)^{O(1)}} = |N|\cdot 2^{(|N|_3)^{O(1)}}$ numbers of the form an $||N||$ bit number multiplied with a 2^k factor for some k.
- So the BPS can be viewed as $|N|\cdot||N||\cdot 2^{(|N|_3)^{O(1)}} = |N|\cdot 2^{(|N|_3)^{O(1)}}$ single bit summands (swallowing the $||N||$ in the O(1) in the exponent).
- Such a number can have at most $|N|\cdot 2^{(|N|_3)^{O(1)}}$ alternations between blocks of 0's and 1's; whereas, f has $\Omega(|N|^2)$ such alternations.

Conclusion

- It would be nice to strengthen Initial.
- Can similar results be obtained for the injective pigeonhole principle?
- It would be interesting to look at propositional translations of this result.