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

Chris Pollett
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$^m_n(f)$:
  \[
  \forall n \forall \bar{z} [n < m \land \exists x < m f(x, \bar{z}) > n \lor \exists x_1, x_2 < m [x_1 \neq x_2 \land f(x_1, \bar{z}) = f(x_2, \bar{z})] \]
  
  If $f$ is a function from $m > n$ into $n$, it is not one-to-one (two points map to the same value).

• sPHP$^m_n(f)$:
  \[
  \forall n \forall \bar{z} [n < m \land \exists y < m \forall x < n f(x, \bar{z}) \neq y] \]
  
  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 $S^{1,2} (:= \text{BASIC + } \Sigma^b_1\text{-LIND})$ 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 $vWPHP^m_n(f)$; whereas, we also have $vWPHP^m_n(\Sigma^b_1(f))$ implies $vPHP^{n\#n}_n(f)$. 
More on Weak Pigeonhole Principles

• For what $f$ can $S^{1,2} (:= \text{BASIC} + \Sigma_{1}^{b} - \text{LIND})$ prove these pigeonhole principles?

Krajíček and Pudlák showed that if $S^{1,2}$ could prove $i\text{WPHP}(\text{PV})$, that is for p-time functions, then RSA is insecure.

Today’s talk will be on for what $f$ can we show $\text{sPHP}_n^m(f)$ is provable in $S^{1,2}$.

The argument probably works with parameters $f$ 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:

  $$\text{Initial} := \text{variables}, 0, S, +, -, \lfloor x \rfloor, \text{PAD}(x, y) := x \cdot 2^{|y|},$$
  $$\text{MSP}(x, y) = \lfloor x/2^y \rfloor, x\#y := 2^{\lfloor \log_2 y \rfloor}.$$  

  - Notice there is no multiplication.

  - This is essentially the initial functions in some of Clote and Takeuti’s papers for $\text{TAC}^0$.

  - 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 \textit{m-length bounded primitive recursion} (m-BPR) if
  \[
  F(0, \bar{x}) = g(\bar{x}) \\
  F(n + 1, \bar{x}) = \min(h(n, \bar{x}, F(n, \bar{x})), r(n, \bar{x})) \\
  f(n, \bar{x}) = F(|t(n, \bar{x})|_m, \bar{x})
  \]
  where \( |x|_0 = x, |x|_{m+1} = ||x||_m \) and \( r \) and \( t \) are terms over Initial.

• From this we define our algebras:
  \( A^m := \text{closure of Initial under composition and m-BPR.} \)
  – \( A^1 \) is the polynomial time functions.
  – We will argue that \( \text{sPHP}^{n\#_n}(A^3) \) is provable in \( S^{1 \frac{1}{2}} \).
Our Approach

• Show in $S^1_2$ that if $x$ is mapped by an $A^3$ function $f:[N] \rightarrow [N\#N]$ then its image must be expressible by a certain kind of series.

• Show that in $S^1_2$ one can define a number $\text{HARD}(N)$ which is hard for this kind of series for any $x < N$.

• This number will be our element not in the range of $f$. 
Our series are called Binary Prefix Series (BPS’s) and can be defined with a predicate:

\[ \text{BPS}(k, N, \bar{x}, S, t) := \]

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 \( s_i = \pm \text{MSP}(x_m, y) \), 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 \( S^{12} \) proves the condition

\[ \forall \bar{x} \exists S \text{ BPS}(k(N), N, \bar{x}, S, f(x)) \]

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 $|.|$ 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 $f(u)$ 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 $\Sigma^b_1$-defined in $S^1_2$ function
  
  $f(N) = \lceil (2^{|\|N\|\| - 1})/3 \rceil$

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

  MSP($x, 0$) · ($2^{k_i}$ factor’s for MSP($x, 0$))
  MSP($x, 1$) · ($2^{k_i}$ factor’s for MSP($x, 1$))
  ...
  MSP($x, |N|$) · ($2^{k_i}$ factor’s for MSP($x, |N|$))

  $-MSP(x, 0)$ · ($2^{k_i}$ factor’s for MSP($x, 0$))
  $-MSP(x, 1)$ · ($2^{k_i}$ factor’s for MSP($x, 1$))
  ...
  $-MSP(x, |N|$) · ($2^{k_i}$ factor’s for MSP($x, |N|$))

• The MSP($x, i$)'s can further be viewed as $|N|$ bit numbers.

• $S^1_2$ can sum the $j$th 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.