This paper demonstrates that the following $\Sigma^b_0$-replacement axioms:

$$\forall i < |x| \exists x < a \phi(i, x) \rightarrow \exists w \forall i < |a| \phi(i, [w]_i)$$

for sharply bounded formulas $\phi$ are unlikely to be provable in three weak arithmetic theories. The first theory considered is a second order theory called $V^0$ which has the usual number axioms for 0, 1, +, $\cdot$, $\leq$, together with induction axioms and comprehension axioms for formulas which use only first order quantifiers. This theory is used to model reasoning about uniform $\mathbf{AC}^0$ circuits, (constant depth, unbounded fan-in AND, OR, NOT circuits). The theory $V^0$ is $\forall \exists \Sigma^b_0$-conservative under $V^0$ together with second order analogs of the replacement axiom. This paper uses the provability of a parity principle to show the two theories are not equal. The next theory considered is $\Delta^b_1$-CR which consists of $\text{BASIC}$ axioms for the symbols $\{0, 1, +, \cdot, <, |x|, (x)i, [x]i, x \# y\}$ together with a comprehension rule which allows one to derive

$$\exists w \forall i < |a|(w)_i = 1 \Leftrightarrow \phi(i),$$

provided $\phi$ is a $\Sigma^b_1$-formula which has been proven equivalent to a $\Pi^b_1$-formula. Here $(x)_i$ projects out the $i$th bit of $x$ and $[x]_i$ projects out the $i$th sequence element of $x$. This language is slightly different from what was used in the original formulation of $\Delta^b_1$-CR given by Johannsen and Pollett [1]. The theory $\Delta^b_1$-CR is RSUV isomorphic to a theory $VTC^0$ which strictly contains $V^0$. The theory $VTC^0$ is typically used to model reasoning about uniform, constant-depth, threshold circuits – the class $\mathbf{TC}^0$. This paper shows that $\Delta^b_1$-CR cannot prove the $\Delta^b_1$-comprehension axioms (as opposed to rules) unless the RSA cryptographic scheme is insecure. As the $\Sigma^b_1$-replacement axioms over $\Delta^b_1$-CR imply the $\Delta^b_1$-comprehension axioms, this implies that $\Sigma^b_1$-replacement is unlikely to be provable in $\Delta^b_1$-CR. The proof of this result actually shows that the theory $\mathbf{PV}$, which is stronger than $\Delta^b_1$-CR, cannot prove the $\Delta^b_1$-comprehension nor the $\Sigma^b_0$-unique replacement axioms unless RSA is insecure. The theory $\mathbf{PV}$ is an equational theory with axioms designed to capture reasoning about polynomial time. It is not equal to $\Delta^b_1$-CR unless polynomial time is equal to uniform $\mathbf{TC}^0$. The theory $\mathbf{PV}$ is the last theory considered by the paper. It is shown that $\mathbf{PV}$ cannot prove the $\Sigma^b_0$-replacements axioms unless factoring is easy. The main proof technique used in the results of this paper is to take the replacement axioms for some hard to invert function $f$. Applying the KPT Witnessing Theorem (a variant of Herbrand’s Theorem) to this axiom for the graph of $f$, gives a finite disjunction of statements from
which an algorithm to invert $f$ can be extracted. This technique seems likely
to be useful in future results.

References