This paper demonstrates that the following Σ_0^{b}-replacement axioms:

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

for sharply bounded formulas ϕ 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 AC^0 circuits, (constant depth, unbounded fan-in AND, OR, NOT circuits). The theory V^0 is $\forall\exists\Sigma_0^{\mathsf{B}}$-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 Δ_1^b-CR which consists of 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 ϕ is a Σ_1^{b}-formula which has been proven equivalent to a Π_1^{b}-formula. Here $(x)_i$ projects out the ith bit of x and $[x]_i$ projects out the ith sequence element of x. This language is slightly different from what was used in the original formulation of Δ_1^b-CR given by Johannsen and Pollett [1]. The theory Δ_1^{b}-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 TC^0. This paper shows that Δ_1^b-CR cannot prove the Δ_1^{b}-comprehension axioms (as opposed to rules) unless the RSA cryptographic scheme is insecure. As the Σ_1^{b}-replacement axioms over Δ_1^{b}-CR imply the Δ_1^{b}-comprehension axioms, this implies that Σ_1^{b}-replacement is unlikely to be provable in Δ_1^{b}-CR. The proof of this result actually shows that the theory PV, which is stronger than Δ_1^b-CR, cannot prove the Δ_1^{b}-comprehension nor the Σ_0^{b}-unique replacement axioms unless RSA is insecure. The theory PV is an equational theory with axioms designed to capture reasoning about polynomial time. It is not equal to Δ_1^{b}-CR unless polynomial time is equal to uniform TC^0. The theory PV is the last theory considered by the paper. It is shown that PV cannot prove the Σ_0^{b}-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

[1] J. Johannsen and C. Pollett. On the Δ_1^{b}-bit comprehension rule. Proceedings of Logic Colloquium 1998. edited by S.R. Buss, P. Hajek, P. Pudlak pp.262–270, A.K.Peters and ASL, 2000.