Comments on Two Definitions of Polynomial Identity Testing Problems

Bin Fu
Department of Computer Science
University of Texas–Pan American
Edinburg, TX 78539, USA
bfu@utpa.edu

November 22, 2013

After the paper "Derandomizing Polynomial Identity over Finite Fields Implies Super-Polynomial Circuit Lower Bounds for NEXP by Bin Fu" appears in ECCC, it has been found that the PIT_q problems constructed in this paper may not exist polynomial time randomized algorithm. There are two versions of PIT problems that are defined below. The author would like to explain their difference and connection to avoid misleading to the computational complexity theory community.

Definition 1. The valuePIT_q problem over a field $F(q)$ is to test if a polynomial $p(x_1, \cdots, x_n)$ computed by an arithmetic circuit over $F(q)$ satisfies $p(a_1, \cdots, a_n) = 0$ for all $a_1, \cdots, a_n \in F(q)$. Let valuePIT_q represent the class of polynomials $p(x_1, \cdots, x_n)$ represented by arithmetic circuits with $p(a_1, \cdots, a_n) = 0$ for all $a_1, \cdots, a_n \in F(q)$.

Definition 2. The coefficientPIT_q problem over a field $F(q)$ is to test if a polynomial $p(x_1, \cdots, x_n)$ computed by an arithmetic circuit over $F(q)$ has the coefficient of each monomial to be zero in its sum of product expansion. Let coefficientPIT_q represent the class of polynomials $p(x_1, \cdots, x_n)$ represented by arithmetic circuits with zero coefficients for all monomials in its sum of product expansion.

Similarly, valuePIT_Z and coefficientPIT_Z are defined over integers Z. All the results of this paper are for valuePIT_q, which is the same as PIT_q defined in Section **??**. The following example shows that the two concepts are different.

Example 1: for every finite field $F(q)$, $p(x) = x(x^{q-1} - 1) = 0$ for every $x \in F(q)$ (see Lemma **??**). Therefore, $p(x) \in \text{valuePIT}_q$, but $p(x) \notin \text{coefficientPIT}_q$.

By Lemma 11 and Lemma 13, we have the following proposition. It shows that valuePIT_q is coNP-hard when q is small.

Proposition 3. *Let $F(q)$ be a finite field of size q. For every instance f of* 3SAT*, there is a polynomial time algorithm that transforms f into a polynomial $p_f(.)$ such that f is unsatisfiable if and only if $p_f(.) \in \text{valuePIT}_q$, and the degree of $p_f(.)$ is $O(qn+m)$, where n is the number of boolean variables in f and m is the number of clauses of f.*

The following proposition follows from Schwartz and Zippel's theorem. It shows that $\text{valuePIT}_Z = \text{coefficientPIT}_Z$, and for a large field $F(q)$, coefficientPIT_q and valuePIT_q contains the same set of polynomials with degree less than q.

Proposition 4.

i. There is a polynomial time randomized algorithm such that given a polynomial $p(.)$ represented by an arithmetic circuit over Z, it decides if $p(.) \in$ coefficientPIT$_Z$. Furthermore, $p(.) \in$ coefficientPIT$_Z$ if and only if $p(.) \in$ valuePIT$_Z$.

ii. There is a polynomial time randomized algorithm such that given a polynomial $p(.)$, represented by an arithmetic circuit, of degree less than q, it decides if $p(.) \in$ coefficientPIT. Furthermore, $p(.) \in$ coefficientPIT if and only if $p(.) \in$ valuePIT (under the condition that the degree of $p(.)$ is less than q).

Example 1 and Proposition 4 show that the condition $degree(p(.)) < q$ is optimal for the equivalence of two polynomial identity notions.

Define the ASIZE/poly to be the class of polynomials of n variables that can be computed by polynomial $n^{O(1)}$ size arithmetic circuits.

For every fixed q, it is known that coefficientPIT$_q \in$ BPP (see "M. Agrawal and S. Biswas: Primality and identity testing via chinese remaindering, J. ACM, 50:429–433, 2003" for example), but it is unknown if valuePIT$_q \in$ BPP. The condition valuePIT$_q \in$ NSUBEXP implies coefficientPIT$_q \in$ NSUBEXP. There is no evidence to support valuePIT$_q \in$ NSUBEXP over any finite field $F(q)$ in complexity theory because it is equivalent to coNP$\subseteq$ NSUBEXP. The separation between NP$^{\text{NP}}$ and NEXP under the condition coNP$\subseteq$ NSUBEXP becomes easy by the nondeterministic time hierarch Theorem. Although Kabanets and Impagliazzo showed that coefficientPIT$_Z \in$ NSUBEXP $\Rightarrow$ NEXP $\not\subseteq$ P/poly or permanent $\notin$ ASIZE/poly, no lower bound implication has been found under the assumption coefficientPIT$_q \in$ P for a finite field $F(q)$.

The paper was submitted to ECCC on November 10, 2013. Three days later, the author realized that valuePIT$_q$ over small field is coNP-hard because co-3SAT, which consists of unsatisfiable instance for 3SAT, can be reduced into a valuePIT$_q$ problem for any fixed field by using the method of this paper.

On November 14, 2013 right before the paper was accepted by ECCC, the author contacted ECCC local office to withdraw it, and was informed on November 15, 2015 to be too late as ECCC needs to maintain the reliability of citations since the paper was already published then.

The author is very grateful to Russel Impagliazzo, Christoph Meinel, Dieter Van Melkebeek, and Ryan Williams for their professional comments and suggestions after the paper appears in ECCC.