Journal of Symbolic Computation 66 (2015) 70–83

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the complexity of Hilbert refutations for partition

S. Margulies [a], S. Onn [b,1], D.V. Pasechnik [c,2]

[a] Department of Mathematics, United States Naval Academy, Annapolis, MD, United States
[b] Industrial Engineering & Management, Technion – Israel Institute of Technology, Haifa, Israel
[c] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore

ARTICLE INFO

Article history:
Received 16 August 2012
Accepted 21 June 2013
Available online 14 February 2014

Keywords:
Hilbert's Nullstellensatz
Linear algebra
Partition

ABSTRACT

Given a set of integers W, the PARTITION problem determines whether W can be divided into two disjoint subsets with equal sums. We model the PARTITION problem as a system of polynomial equations, and then investigate the complexity of a Hilbert's Nullstellensatz refutation, or certificate, that a given set of integers is not partitionable. We provide an explicit construction of a minimum-degree certificate, and then demonstrate that the PARTITION problem is equivalent to the determinant of a carefully constructed matrix called the partition matrix. In particular, we show that the determinant of the partition matrix is a polynomial that factors into an iteration over all possible partitions of W.

Published by Elsevier Ltd.

1. Introduction

The NP-complete problem PARTITION (Garey and Johnson, 1979) is the question of deciding whether or not a given set of integers $W = \{w_1, \ldots, w_n\}$ can be broken into two sets, I and $W \setminus I$, such that the sums of the two sets are equal, or that $\sum_{w \in I} w = \sum_{w \in W \setminus I} w$. Since it is widely believed that NP $\neq$ coNP, it is interesting to study various types of *refutations*, or certificates for the *non*-existence of a partition in a given set W.

In this paper, we study the certificates provided by Hilbert's Nullstellensatz (see Alon, 1992; Alon and Tarsi, 1992; De Loera et al., 2009b; Lovász, 1994; Onn, 2004 and references therein). Given

E-mail addresses: margulie@usna.edu (S. Margulies), onn@ie.technion.ac.il (S. Onn), dima@ntu.edu.sg (D.V. Pasechnik).
[1] Research of this author was supported in part by a grant from the Israel Science Foundation.
[2] Research of this author was supported in part by Singapore MOE Tier 2 Grant MOE2011-T2-1-090 (ARC 19/11).

http://dx.doi.org/10.1016/j.jsc.2013.06.005
0747-7171/Published by Elsevier Ltd.

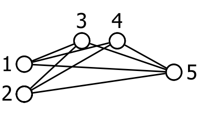
an algebraically-closed field $\mathbb{K}$ and a set of polynomials $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$, Hilbert's Nullstellensatz states that the system of polynomial equations $f_1 = f_2 = \cdots = f_s = 0$ has *no* solution if and only if there exist polynomials $\beta_1, \dots, \beta_s \in \mathbb{K}[x_1, \dots, x_n]$ such that $1 = \sum_{i=1}^{s} \beta_i f_i$. We measure the complexity of a given certificate in terms of the size of the β coefficients, since these are the unknowns we must discover in order to demonstrate the *non*-existence of a solution to $f_1 = f_2 = \cdots = f_s = 0$. Thus, we measure the degree of a Nullstellensatz certificate as $d = \max\{\deg(\beta_1), \dots, \deg(\beta_s)\}$.

There is a well-known connection between Hilbert's Nullstellensatz and a particular sequence of linear algebra computations. These sequences have been studied from both a theoretical perspective (Buss and Pitassi, 1996; De Loera et al., 2009b), and a computational perspective (De Loera et al., 2009a, 2011). When the polynomial ideal contains $x_i^2 - x_i$ for each variable (thus forcing the variety to contain only 0/1 points), these sequences have also been explored as algebraic proof systems (Beame et al., 1996; Clegg et al., 1996; Impagliazzo et al., 1999; Razborov, 1998). Additionally, D. Grigoriev demonstrates a linear lower bound for the knapsack problem in Grigoriev (2001) (see also Grigoriev et al., 2002), and Buss and Pitassi (1996) show that a polynomial system loosely based upon the "pigeon-hole principle" requires a $\lfloor \log n \rfloor - 1$ Nullstellensatz degree certificate. However, when the system of polynomial equations $f_1, \dots, f_s$ models an NP-complete problem, the degree d is likely to grow at least linearly with the size of the underlying NP-complete instance (Margulies, 2008). In other words, as long as P $\neq$ NP, the certificates should be hard to find (i.e., the size of the linear systems involved should be exponential in the size of the underlying instance), and as long as NP $\neq$ coNP, the certificates should be hard to verify (i.e., the certificates should contain an exponential number of monomials).

For example, consider the NP-complete problem of finding an independent set of size k in a graph G. Recall that an independent set is a set of pairwise non-adjacent vertices. This problem was modeled by Lovász (1994) as a system of polynomial equations as follows:

$$\begin{array}{ll} x_i^2 - x_i = 0, & \text{for every vertex } i \in V(G), \\ x_i x_j = 0, & \text{for every edge } (i,j) \in E(G), \end{array} \quad \text{and} \quad -k + \sum_{i=1}^{n} x_i = 0.$$

Clearly, this system of polynomial equations has a solution if and only if the underlying graph G has an independent of size k. For example, consider the Turán graph $T(5,3)$. By inspection, we see that size of the largest independent set in $T(5,3)$ is two. Therefore, there is *no* independent set of size three, and using the connection between Hilbert's Nullstellensatz and linear algebra (described more thoroughly in Section 3), De Loera et al. (2009b) produce the following certificate:



Turán graph $T(5,3)$

$$\begin{aligned} &\left(\frac{1}{3}x_4 + \frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_3 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_4 + \left(\frac{1}{3}x_2 + \frac{1}{3}\right)x_1x_5 \\ &\quad + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_2x_3 + \left(\frac{1}{3}\right)x_2x_4 + \left(\frac{1}{3}\right)x_2x_5 \\ &\quad + \left(\frac{1}{3}x_4 + \frac{1}{3}\right)x_3x_5 + \left(\frac{1}{3}\right)x_4x_5 + \left(\frac{1}{3}x_2 + \frac{1}{6}\right)(x_1^2 - x_1) \\ &\quad + \left(\frac{1}{3}x_1 + \frac{1}{6}\right)(x_2^2 - x_2) + \left(\frac{1}{3}x_4 + \frac{1}{6}\right)(x_3^2 - x_3) \\ &\quad + \left(\frac{1}{3}x_3 + \frac{1}{6}\right)(x_4^2 - x_4) + \left(\frac{1}{6}\right)(x_5^2 - x_5) \\ &\quad + \underbrace{\left(-\frac{1}{3}(x_1x_2 + x_3x_4) - \frac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5) - \frac{1}{3}\right)}_{\beta_1} \\ &\quad \times (x_1 + x_2 + x_3 + x_4 + x_5 - 3) = 1. \end{aligned}$$

The combinatorial interpretation of this algebraic identity is unexpectedly clear: the size of the largest independent set is the degree of the Nullstellensatz certificate (i.e., the largest monomial