Algebraic complexity in finite fields

Author(s):
Ganz, Jürg Werner

Publication Date:
1994

Permanent Link:

https://doi.org/10.3929/ethz-a-001369108 →

Diss. ETH No. 10867

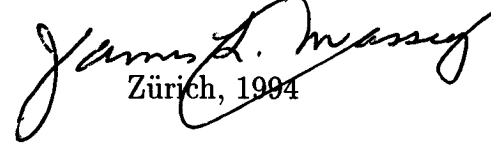
Algebraic Complexity in Finite Fields

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZÜRICH
for the degree of
Doctor of Technical Sciences

presented by

JÜRG WERNER GANZ
dipl. El.-Ing. ETH
born May 17, 1963
citizen of Zürich and Dorf b. Andelfingen ZH

accepted on the recommendation of
Prof. Dr. J.L. Massey, referee
Prof. Dr. P. Camion, co-referee



Zürich, 1994

Abstract

Functions mapping a vector of elements of a finite field to another vector of elements of the same field are studied by using the concept of straight-line algorithms and the corresponding algebraic complexity that counts additions and multiplications in the field. If the operations are in GF(2), then this complexity measure is essentially the Boolean circuit complexity.

A central role in these considerations is played by binary representations of finite fields, which are introduced and their algebraic complexity studied. A method of surrogate computation is introduced to prove several relations that give insight into binary representations. Several applications of these results are given. The circuit complexity of Zech's logarithm is shown to be closely related to the circuit complexity of the discrete logarithm problem applied in public-key cryptography. For any finite field with characteristic p such that $p-1$ has only small prime factors, it is proved that algebraic complexity in this field is essentially equivalent to circuit complexity. Further, an efficient new algorithm to factor a polynomial over a finite field is presented that exploits a binary representation of the field; the algorithm is shown to be of practical value, e.g., in decoders for Reed-Solomon codes.

New algorithms to evaluate polynomials are proposed. They exploit the fact that the coefficients of the polynomials are in a finite field. With respect to the number of operations (additions and multiplications), these algorithms outperform all previously known algorithms for many interesting cases. These algorithms for evaluating polynomials are used to upperbound the algebraic complexity of functions. Tight bounds on the maximum complexity of functions are obtained, even when the function table is only partially defined. The most difficult functions are also studied with respect to multiplicative and additive complexity, i.e., the minimum number of multiplications and additions,

respectively, needed. For many types of finite fields, the maximum additive complexity is proved to be only about the square root of the maximum algebraic complexity and in this respect is very similar to the maximum multiplicative complexity. It is shown that, for any function, additive, multiplicative and algebraic complexity are closely related.

Several new lower bounds on the algebraic complexity of specific functions are given, but these lower bounds are only slightly better than trivial lower bounds and not strong enough to have new practical consequences.

Kurzfassung

Funktionen werden untersucht, die einen Vektor von Elementen aus einem endlichen Körper in einen anderen Vektor von Elementen desselben Körpers abbilden. Dabei wird das Konzept von "straight-line" Algorithmen und die dazugehörige algebraische Komplexität, welche Additionen und Multiplikationen im Körper zählt, benützt. Falls die Operationen in GF(2) sind, dann ist dieses Komplexitätsmass im wesentlichen die Boolesche Schaltungskomplexität.

Eine wichtige Rolle in diesen Untersuchungen haben binäre Darstellungen von endlichen Körpern, welche eingeführt und bezüglich ihrer algebraischen Komplexität untersucht werden. Eine Methode von Ersatzberechnungen wird eingeführt, um verschiedene Zusammenhänge zu beweisen, die Einsicht in die binären Darstellungen geben. Einige Anwendungen dieser Resultate werden vorgestellt. Es wird gezeigt, dass die Schaltungskomplexität von Zech's Logarithmus eng mit der Schaltungskomplexität desjenigen diskreten Logarithmus Problems zusammenhängt, welches in der "public-key" Kryptographie benützt wird. Für irgendeinen endlichen Körper mit Charakteristik p, wobei $p-1$ nur kleine Primfaktoren hat, wird bewiesen, dass die algebraische Komplexität in diesem Körper im wesentlichen der Schaltungskomplexität entspricht. Weiter wird ein neuer, effizienter Algorithmus vorgestellt, der Polynome über einem endlichen Körper faktorisiert. Dieser Algorithmus nützt eine binäre Darstellung des Körpers aus und erweist sich auch für praktische Anwendungen als interessant, z.B. bei der Decodierung von Reed-Solomon Codes.

Neue Algorithmen zur Auswertung von Polynomen werden vorgeschlagen. Sie verwenden die Tatsache, dass die Koeffizienten der Polynome aus einem endlichen Körper sind. Bezüglich der Anzahl benötigter Operationen (Additionen und Multiplikationen) sind diese Algorithmen in vielen wichtigen Fällen allen anderen bekannten Algo-

rithmen vorzuziehen. Diese Algorithmen zur Auswertung von Polynomen werden benützt, um obere Schranken für die algebraische Komplexität von Funktionen herzuleiten. Enge Schranken für die maximale Komplexität von Funktionen werden gezeigt, auch wenn die Funktionstabellen nur teilweise definiert sind. Die schwierigsten Funktionen werden auch bezüglich multiplikativer und additiver Komplexität untersucht, d.h. bezüglich der minimalen Anzahl benötigter Multiplikationen, beziehungsweise Additionen. Für viele Arten von endlichen Körpern wird gezeigt, dass die maximale additive Komplexität nur etwa die Quadratwurzel der maximalen algebraischen Komplexität ist und dass sie sich in dieser Beziehung ähnlich wie die maximale multiplikative Komplexität verhält. Es wird bewiesen, dass die additive, multiplikative und algebraische Komplexität einer beliebigen Funktion eng miteinander verknüpft sind.

Einige neue untere Schranken für die algebraische Komplexität von spezifischen Funktionen werden hergeleitet. Diese untere Schranken sind jedoch nur leicht besser als triviale untere Schranken und sind nicht stark genug, um neue Konsequenzen für praktische Anwendungen zu haben.