Discrete Mathematics and Theoretical Computer Science **6**, 2003, 0041–044

A Note on Set Systems with no Union of Cardinality 0 Modulo m

Vince Grolmusz

Department of Computer Science, Eötvös University, H-1117 Budapest, HUNGARY.
e-mail: grolmusz@cs.elte.hu

received September, 2001, *revised October, 2002*, *accepted March, 2003*.

Alon, Kleitman, Lipton, Meshulam, Rabin and *Spencer* (Graphs. Combin. 7 (1991), no. 2, 97-99) proved that for any hypergraph $\mathcal{F} = \{F_1, F_2, \ldots, F_{d(q-1)+1}\}$, where q is a prime-power, and d denotes the maximum degree of the hypergraph, there exists an $\mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F \in \mathcal{F}_0} F| \equiv 0 \pmod q$. The main tool of the proof was a one-to-one correspondence between hypergraphs and polynomials. We give a direct, alternative proof to this correspondence, and also review its implications for set-systems following from the result of *Barrington, Beigel* and *Rudich* (Comput. Complexity, 4 (1994), 367-382) for certain mod 6 polynomials.

Keywords: Set systems, composite modulus, polynomials over rings

1 Introduction

Alon, Kleitman, Lipton, Meshulam, Rabin and *Spencer* [1] gave the following definition:

Definition 1 ([1]) *For integers $d, m \geq 1$, let $f_d(m)$ denote the smallest t such that for any hypergraph $\mathcal{F} = \{F_1, F_2, \ldots, F_t\}$ with maximum degree d there exists a non-empty $\mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F \in \mathcal{F}_0} F| \equiv 0 \pmod m$*

Baker and *Schmidt* [2] defined the following quantity:

Definition 2 *For integers $d, m \geq 1$, let $g_d(m)$ denote the smallest t such that for any polynomial $h \in Z[x_1, x_2, \ldots, x_t]$ of degree d, satisfying $h(\mathbf{0}) = 0$, there exists an $\mathbf{0} \neq \varepsilon \in \{0,1\}^n$, such that $h(\varepsilon) \equiv 0 \pmod m$.*

The following theorem was proven in [1]:

Theorem 3 ([1])

$$f_d(m) = g_d(m)$$

In the next section we give a natural one-to-one correspondence between polynomials and hypergraphs, proving Theorem 3.

For p prime, and α positive integer it is known ([1], [2], [4]) that $g_d(p^\alpha) = d(p^\alpha - 1) + 1$, so we obtain

1365–8050 © 2003 Discrete Mathematics and Theoretical Computer Science (DMTCS), Nancy, France

Corollary 4 ([1]) *For $\mathcal{F} = \{F_1, F_2, \ldots, F_{d(q-1)+1}\}$, where q is a prime-power, and d denotes the maximum degree of the hypergraph, there exists an $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F\in\mathcal{F}_0} F| \equiv 0 \pmod q$.*

This corollary is a generalization of the undergraduate exercise that from arbitrary m integers, one can choose a non-empty subset, which adds up to 0 modulo m (the $d = 1$ case).

In 1991, *Barrington, Beigel* and *Rudich* [3] gave an explicit construction for polynomials modulo $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, showing that

$$g_d(m) = \Omega(d^r).$$

Since the proof of Theorem 3 (both the original and ours in the next section) gives explicit constructions for hypergraphs from polynomials, the following corollary holds:

Corollary 5 *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$. Then there exists an explicitly constructible hypergraph $\mathcal{F}$ of maximum degree d, such that $|\mathcal{F}| = \Omega(d^r)$ and for each $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$ it is satisfied that $|\bigcup_{F\in\mathcal{F}_0} F| \not\equiv 0 \pmod m$.*

The authors of [1] gave a doubly-exponential upper bound on $f_d(m)$, which was based on a Ramsey-theoretic bound of [2]. More recently, *Tardos* and *Barrington* [4] showed that

$$f_d(m) = \exp(O(d^{r-1})).$$

2 Correspondence between polynomials and hypergraphs

We give here a short and direct proof for Theorem 3. Let Q denote the set of rationals. It is well known that the set of functions $\{f : \{0,1\}^t \to Q\}$ forms a 2^t-dimensional vector space over the rationals. One useful basis of this vector space is the set of OR-functions $\{\bigvee_{i\in I} x_i : I \subset \{1,2,\ldots,t\}\}$, where

$$\bigvee_{i\in I} x_i = 1 - \prod_{i\in I}(1 - x_i).$$

It is easy to see that any integer-valued function on the hypercube can be written as the integer-coefficient linear combination of these OR-functions. Moreover, if the function is a degree-d polynomial, then it is enough to use OR functions with $|I| \le d$. If we consider modulo m polynomials, then the coefficients can be restricted to the set $\{0,1,2,\ldots,m-1\}$. It will be convenient to view modulo m polynomials as the sum of several OR functions with coefficient 1; instead of multiplying an OR function with a coefficient a we will add it up exactly a times.

Consequently, our degree-d modulo m polynomial has the following form:

$$h = S_1 + S_2 + \cdots + S_\ell, \tag{1}$$

where S_i is an OR-function of degree at most d.

Now we are ready to define the one-to-one correspondence between degree-d modulo m polynomials without non-trivial zeroes on the hypercube and hypergraphs, without non-empty subhypergraphs of modulo-m union-size 0. Let h be a degree-d polynomial written in form (1), and define hypergraph $\mathcal{F} = \{F_1, F_2, \ldots, F_t\}$, where $F_i = \{S_j : x_i$ appears as a variable in $S_j\}$. Clearly, the degree of this hypergraph is at most the degree of h that is, d.

On the other hand, for a hypergraph $\mathcal{F} = \{F_1, F_2, \ldots, F_t\}$ on the ground-set $\{v_1, v_2, \ldots, v_\ell\}$, let us define $h(x_1, x_2, \ldots, x_t) = S_1 + S_2 + \cdots + S_\ell$, where

$$S_j = \bigvee_{i: v_j \in F_i} x_i.$$

Obviously, the degree of h is at most the degree of $\mathcal{F}$.

Now we state that $\mathcal{F}$ has a non-empty subhypergraph with union-size 0 modulo m if and only if there exists a $\mathbf{0} \neq \mathbf{x} : h(\mathbf{x}) \equiv 0 \pmod{m}$. The proof is as follows: For $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ let us denote $I(\mathbf{x}) = \{i : x_i = 1\}$. Then $S_j(\mathbf{x}) = 1$ if $S_j \in \bigcup_{i \in I(\mathbf{x})} F_i$, and $S_j(\mathbf{x}) = 0$ otherwise. Thus $h(\mathbf{x}) = |\bigcup_{i \in I(\mathbf{x})} F_i|$ holds for all $\mathbf{x} \in \{0,1\}^n$. In particular, evaluations of h and union-sizes of subhypergraphs in $\mathcal{F}$ become divisible by m simultaneously. $\square$

Acknowledgment.

The author is grateful for the anonymous referee for his/her suggestions clarifying the correspondence between polynomials and hypergraphs. The author also acknowledges the partial support of research grants EU FP5 IST FET No. IST-2001-32012, OTKA T030059.

References

[1] N. Alon, D. Kleitman, R. Lipton, R. Meshulam, M. Rabin, and J. Spencer. Set systems with no union of cardinality 0 modulo m. *Graphs and Combinatorics*, 7:97–99, 1991.

[2] R. Baker and W. Schmidt. Diophantine problems in variables restricted to the values 0 and 1. *Journal of Number Theory*, 12:460–486, 1980.

[3] D. A. M. Barrington, R. Beigel, and S. Rudich. Representing Boolean functions as polynomials modulo composite numbers. *Comput. Complexity*, 4:367–382, 1994. Appeared also in *Proc. 24th Ann. ACM Symp. Theor. Comput.*, 1992.

[4] G. Tardos and D. A. M. Barrington. A lower bound on the MOD 6 degree of the OR function. *Comput. Complexity*, 7:99–108, 1998.