

L-balancing families

Gábor Hegedűs
Óbuda University
Bécsi út 96, Budapest, Hungary, H-1037
hegedus.gabor@nik.uni-obuda.hu

May 5, 2021

Abstract
P. Hrubeš, S. Natarajan Ramamoorthy, A. Rao and A. Yehudayoff proved the following result:
Let \( p \) be a prime and let \( f \in \mathbb{F}_p[x_1, \ldots, x_{2p}] \) be a polynomial. Suppose that \( f(v_F) = 0 \) for each \( F \subseteq [2p] \), where \( |F| = p \) and that \( f(0) \neq 0 \). Then \( \deg(f) \geq p \).

We prove here the following generalization of their result.

Let \( p \) be a prime and \( q = p^\alpha > 1, \alpha \geq 1 \). Let \( n > 0 \) be a positive integer and \( q - 1 \leq d \leq n - q + 1 \) be an integer. Let \( \mathbb{F} \) be a field of characteristic \( p \). Suppose that \( f(v_F) = 0 \) for each \( F \subseteq [n] \), where \( |F| = d \) and \( \deg(f) \leq q - 1 \). Then \( f(v_F) = 0 \) for each \( F \subseteq [n] \), where \( |F| \equiv d \pmod{q} \).

Let \( t = 2d \) be an even number and \( L \subseteq [d - 1] \) be a given subset. We say that \( F \subseteq 2^\lfloor t \rfloor \) is an \( L \)-balancing family if for each \( F \subseteq [t] \), where \( |F| = d \) there exists a \( G \subseteq [n] \) such that \( |F \cap G| \in L \).

We give a general upper bound for the size of an \( L \)-balancing family.

1 Introduction

First we introduce some notations.

Let \( n \) be a positive integer and let \([n]\) stand for the set \( \{1, 2, \ldots, n\} \). The family of all subsets of \([n]\) is denoted by \( 2^n \). For an integer \( 0 \leq d \leq n \)
we denote by \( \binom{[n]}{d} \) the family of all \( d \) element subsets of \([n]\), and \( \binom{[n]}{\leq d} = \binom{[n]}{0} \cup \ldots \cup \binom{[n]}{d} \) the subsets of size at most \( d \).

Let \( \mathbb{F} \) be a field. \( \mathbb{F}[x_1, \ldots, x_n] \) denotes the ring of polynomials in variables \( x_1, \ldots, x_n \) over \( \mathbb{F} \). Let \( S = \mathbb{F}[x_1, \ldots, x_n] \). In this paper \( \mathbb{F} \) will be a finite prime field \( \mathbb{F}_p \).

In the following \( v_F \in \{0, 1\}^n \) denotes the characteristic vector of a set \( F \subseteq [n] \). For a family of subsets \( F \subseteq 2^{[n]} \), let

\[
V(F) = \{ v_F : F \in F \} \subseteq \{0, 1\}^n \subseteq \mathbb{F}^n.
\]

It is natural to consider the ideal \( I(V(F)) \):

\[
I(V(F)) := \{ f \in S : f(v) = 0 \text{ whenever } v \in V(F) \}.
\]

Denote by \( \mathbb{F}[x_1, \ldots, x_n]_{\leq s} \) the vector space of all polynomials over \( \mathbb{F} \) with degree at most \( s \).

Let \( I \) be an ideal of the ring \( S = \mathbb{F}[x_1, \ldots, x_n] \). Let \( h_{S/I}(m) \) denote the dimension over \( \mathbb{F} \) of the factor-space \( \mathbb{F}[x_1, \ldots, x_n]_{\leq m}/(I \cap \mathbb{F}[x_1, \ldots, x_n]_{\leq m}) \) (see [3] Section 9.3). The Hilbert function of the algebra \( S/I \) is the sequence \( h_{S/I}(0), h_{S/I}(1), \ldots \).

It is easy to verify that in the special case when \( I = I(V(F)) \) for some set system \( F \subseteq 2^{[n]} \), the number \( h_F(m) := h_{S/I}(m) \) is the dimension of the space of functions from \( V(F) \) to \( \mathbb{F} \) which can be represented as polynomials of degree at most \( m \).

Let \( p \) be a prime and \( n > 1 \), \( 0 \leq d \leq n \) be integers. Let \( q = p^\alpha, \alpha \geq 1 \). Define the family of sets

\[
\mathcal{F}(d, q) = \{ K \subseteq [n] : |K| \equiv d \pmod{q} \}.
\]

I proved the following result in [11].

**Lemma 1.1** Let \( p \) be a prime and let \( f \in \mathbb{F}_p[x_1, \ldots, x_{4p}] \) be a polynomial. Suppose that \( f \in I(V(\binom{[4p]}{2p})) \) and that \( f \notin I(V(\binom{[3p]}{3p})) \). Then \( \deg(f) \geq p \).

My proof used a combination of Gröbner basis methods and linear algebra. Srinivasan gave a simpler proof which combined Fermat’s little Theorem with linear algebra (see [5]). Alon found a third proof based on the Combinatorial Nullstellensatz (see [3]).

P. Hrubeš, S. Natarajan Ramamoorthy, A. Rao and A. Yehudayoff proved a similar result to our Lemma 1.1.
Lemma 1.2 Let $p$ be a prime and let $f \in \mathbb{F}_p[x_1, \ldots, x_{2p}]$ be a polynomial. Suppose that $f \in I(V({\binom{n}{p}}))$ and that $f(0) \neq 0$. Then $\deg(f) \geq p$.

Let $m$ be a positive integer and $n$ be a positive even integer. We say that a proper non-empty subsets $S_1, \ldots, S_m$ are a balancing set of family if for every $X \in \binom{n}{n/2}$ there is an index $i \in [k]$ such that $|S_i \cap X| = |S_i|/2$.

Let $n$ be a positive even integer. We define now $L$-balancing families. Let $n = 2d$ be an even number and $L \subseteq [d - 1]$ be a given subset. We say that $F \subseteq 2^{[n]}$ is an $L$-balancing family if for each $F \in \binom{n}{d}$ there exists a $G \subseteq [n]$ such that $|F \cap G| \in L$.

We prove the following general upper bound for the size of an $L$-balancing family. Our proof is based completely on Lemma 1.2.
Theorem 1.5 Let $p$ be a prime. Let $n := 2p$ and $L \subseteq \{p - 1\}$ be a given subset. Define $s := |L|$. Let $\mathcal{F} \subseteq 2^n$ be an $L$-balancing family. Then
\[ m := |\mathcal{F}| \geq \frac{n}{2s}. \]

We prove our results in Section 2.

2 Proofs

Proof of Theorem [1.3]: It follows from the definition of the Hilbert function that
\[ h_{\mathcal{F}}(m) = \text{dim}(S_{\leq m}) - \text{dim}(I(\mathcal{F})_{\leq m}) \]
and
\[ h_{\mathcal{G}}(m) = \text{dim}(S_{\leq m}) - \text{dim}(I(\mathcal{G})_{\leq m}). \]
Since $h_{\mathcal{F}}(m) = h_{\mathcal{G}}(m)$, hence $\text{dim}(I(\mathcal{F})_{\leq m}) = \text{dim}(I(\mathcal{G})_{\leq m})$.
But $\mathcal{F} \subseteq \mathcal{G}$ implies that $I(\mathcal{G})_{\leq m} \subseteq I(\mathcal{F})_{\leq m}$, consequently $I(\mathcal{F})_{\leq m} = I(\mathcal{G})_{\leq m}$.  

Proof of Theorem [1.4]: We gave an alternative proof in [12] Corollary 3.1 using Gröbner basis theory for Wilson’s theorem about the Hilbert function of complete uniform families.

Theorem 2.1 (Wilson, [16]) Let $0 \leq d \leq n$, $0 \leq m \leq \min\{d, n - d\}$, and $\mathbb{F}$ be an arbitrary field. Then we have
\[ h_{\binom{n}{m}}(m) = \binom{n}{m}. \]

We determined the Hilbert function of the set system $\mathcal{F}(d, q)$ in [10] Corollary 4.5.

Theorem 2.2 Let $p$ be a prime and $q = p^\alpha > 1, \alpha \geq 1$. Let $\mathbb{F}$ be a field of characteristic $p$. Let $n > 0$, $0 \leq d \leq n$ be integers and define $r = \min\{d, n - d\}$. Let $h_{\mathcal{F}(d, q)}(m)$ denote the Hilbert function of $\mathbb{F}[x]/I(V(\mathcal{F}(d, q)))$. Then
\[ h_{\mathcal{F}(d, q)}(m) = \sum_{i=0}^{\left\lfloor \frac{m}{q} \right\rfloor} \binom{n}{m - iq}. \]
if $0 \leq m \leq r$, and

$$h_{\mathcal{F}(d,q)}(m) = \sum_{i=-\left\lfloor \frac{n-m}{q} \right\rfloor}^{\left\lceil \frac{n-r}{q} \right\rceil} \binom{n}{r+iq} - \sum_{i=1}^{\left\lfloor \frac{n-m}{q} \right\rfloor} \binom{n}{m+iq}$$

if $m > r$.

Let $q-1 \leq d \leq n-q+1$ be an integer. Suppose that $f \in I(V(\binom{[n]}{d})_{\leq q-1})$. It follows from Theorem 2.1 and Theorem 2.2 that $h(\binom{[n]}{d})(q-1) = h_{\mathcal{F}(d,q)}(q-1) = \binom{n}{q-1}$.

Hence Theorem 1.3 gives us that $f \in I(V(\mathcal{F}(d,q)))_{\leq q-1}$.

Proof of Theorem 1.5

Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ be an $L$-balancing family and let $v_i := v_{F_i}$ denote the characteristic vector of $F_i$ for each $1 \leq i \leq m$.

Consider the polynomial

$$P(x) := \prod_{i=1}^{m} \prod_{\ell \in L} (x \cdot v_i - \ell) \in \mathbb{F}_p[x].$$

Here $\cdot$ denotes the usual scalar product. Clearly $\deg(P) \leq ms$.

Then $P(0) = (\prod_{\ell \in L} \ell)^m \neq 0$. On the other hand, $P(v_G) = 0$ for each $G \in \binom{[n]}{p}$, because $\mathcal{F}$ is an $L$-balancing family.

Hence it follows from Lemma 1.2 that $\deg(P) \geq p$ and we get that $p \leq ms$.

References

[1] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, American Mathematical Society, 1994.

[2] R.P. Anstee, L. Rónyai, A. Sali, Shattering news, *Graphs and Combinatorics* 18 (2002), 59–73.

[3] N. Alon, Problems and results in Extremal Combinatorics–IV. arXiv preprint [arXiv:2009.12692] (2020).
[4] N. Alon, E. E. Bergmann, D. Coppersmith and A. M. Odlyzko, Balancing sets of vectors. *IEEE Trans. on Information Theory*, 34(1), 128-130 (1988).

[5] N. Alon, Kumar, M., and B. L. Volk, (2020). Unbalancing sets and an almost quadratic lower bound for syntactically multilinear arithmetic circuits. *Combinatorica*, 40(2), 149-178.

[6] T. Becker, V. Weispfenning, *Gröbner bases - a computational approach to commutative algebra*, Springer-Verlag, Berlin, Heidelberg, 1993.

[7] A. M. Cohen, H. Cuypers, H. Sterk (eds.), *Some Tapas of Computer Algebra*, Springer-Verlag, Berlin, Heidelberg, 1999.

[8] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Springer-Verlag, Berlin, Heidelberg, 1992.

[9] K. Friedl, L. Rónyai, Order-shattering and Wilson’s theorem, to appear, *Discrete Mathematics*.

[10] B. Felszeghy, G. Hegedüs, and L. Rónyai (2009). Algebraic properties of modulo $q$ complete $\ell$-wide families. *Comb., Prob. and Computing*, 18(3), 309-333.

[11] G. Hegedüs (2010). Balancing sets of vectors. Studia Scientiarum Mathematicarum Hungarica, 47(3), 333-349.

[12] G. Hegedüs, L. Rónyai, Gröbner bases for complete uniform families, *J. of Algebraic Combinatorics* 17 (2003), 171–180.

[13] G. Hegedüs, L. Rónyai, Standard monomials for $q$-uniform and a conjecture of Babai and Frankl, *Central European Journal of Mathematics* 1 (2003), 198–207. [http://www.cesj.com/mathematics.html](http://www.cesj.com/mathematics.html)

[14] P. Hrubeš, S. Natarajan Ramamoorthy, A. Rao and A. Yehudayoff, Lower bounds on balancing sets and depth-2 threshold circuits. In 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. (2019).
[15] S. Srinivasan, A robust version of Hegedüs’s lemma, with applications. In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (pp. 1349-1362) (2020).

[16] R.M. Wilson, A diagonal form for the incidence matrices of $t$-subsets vs. $k$ subsets, *Europ. J. Combin.* **11**(1990), 609–615.