A lemma on the randomness of d-th powers in $GF(q)$, $d|q-1$

P. Sziklai*

Abstract

In this short note a theorem on the random-like behaviour of d-th powers in $GF(q)$ is proved, for $d|q-1$. It is a common generalization of a result by Szőnyi [4] and another by Babai, Gál and Wigderson [1].

1 Introduction

In this paper we prove a theorem, which is a common generalization of a result of Szőnyi [4] and another by Babai, Gál and Wigderson [1]. It is interesting in itself, applications can be found in future. Its moral, roughly speaking, is that under some light and natural conditions, it is a "random event of probability $\frac{1}{d}$" being a d-th power in $GF(q)$, where d is a divisor of $q-1$.

In fact this theorem is a consequence of the character sum version of Weil's estimate. In order to formulate it, we need a

Definition 1.1. *Let $f_1(x), \ldots, f_m(x) \in GF(q)[x]$ be given polynomials. We say that their system is d-*power independent*, if no partial product $f_{i_1}^{s_1} f_{i_2}^{s_2} \ldots f_{i_j}^{s_j}$ $(1 \le j \le m;$ $1 \le i_1 < i_2 < \ldots < i_j \le m;$ $1 \le s_1, s_2, \ldots, s_j \le d-1)$ can be written as a constant multiple of a d-th power of a polynomial.*

Equivalently, one may say that if any product $f_{i_1}^{s_1} f_{i_2}^{s_2} \ldots f_{i_j}^{s_j}$ is a constant multiple of a d-th power of a polynomial, then this product is 'trivial', i.e. for all the exponents $d|s_i$, $i = 1, \ldots, j$. Now

*Research was partially supported by OTKA F030737, D32817 and Eötvös grants.
Received by the editors February 2000.
Communicated by J. Thas.

Theorem 1.2. *Let $f_1(x),\dots,f_m(x)\in GF(q)[x]$ be a set of d-power independent polynomials, where $d|(q-1)$. If*

$$d^{m-1}\sum_{i=1}^{m}\deg(f_i)<\frac{q+\sqrt{q}(d^m-1)}{\frac{d(d-1)}{2}\sqrt{q}+1},$$

then there is an $x_0\in GF(q)$ such that every $f_i(x_0)$ is a d-th power in $GF(q)$ for every $i=1,\dots,m$. More precisely, if we denote the number of these x_0-s by N, then

$$|N-\frac{q}{d^m}|\le\left(\frac{d-1}{2}\sqrt{q}+\frac{1}{d}\right)\sum_{i=1}^{m}\deg(f_i)-\sqrt{q}\left(1-\frac{1}{d^m}\right).$$

For the sake of simplicity one can say that if $\sum_{i=1}^{m}\deg(f_i)<\frac{2\sqrt{q}}{d^m(d-1)}$ then $|N-\frac{q}{d^m}|\le\frac{d-1}{2}\sqrt{q}\sum_{i=1}^{m}\deg(f_i)$, if $d^m\ge 4$.

Note that this theorem implies that, under some natural conditions, one can solve a system of equations

$$\chi_d(f_i(x))=\delta_i\qquad(i=1,\dots,m),$$

where the δ_i-s are d-th complex roots of unity, and χ_d is the multiplicative character of order d. So 'the d-th power behaviour' can be prescribed if the polynomials are 'independent'. It can be interpreted as 'being a d-th power' is like a random event of probability $\frac{1}{d}$.

Some words about the condition $d|(q-1)$: as the d-th and the g.c.d.$(d,q-1)$-th powers are the same, if $d|q-1$ were not the case, one may apply the lemma with g.c.d.$(d,q-1)$ instead of d.

We remark that Szőnyi [4] proved this theorem for $d=2$, while L. Babai, A. Gál and Wigderson [1] for linear polynomials.

We will need

Result 1.3 (character sum version of Weil's estimate, [2], Thm. 5.41) *Let $f(x)$ be a polynomial over $GF(q)$ and r the number of distinct roots of f in its splitting field. If χ_e is a multiplicative character (of order e)of $GF(q)$ and $f(x)\ne cg(x)^e$, then*

$$|\sum_{x\in GF(q)}\chi_e(f(x))|\le(r-1)\sqrt{q}.$$

■

2 The proof

Proof of Theorem 1.2: First note that we use the definition $\chi(x)=\chi_d(x)=x^{\frac{q-1}{d}}$. Let $\{\varepsilon_0=1,\varepsilon_1,\varepsilon_2,\dots,\varepsilon_{d-1}\}$ be the set of d-th complex roots of unity. Define the following expression:

$$\begin{aligned}H&=\sum_{x\in GF(q)}\prod_{i=1}^{m}(\chi(f_i(x))-\varepsilon_1)(\chi(f_i(x))-\varepsilon_2)\dots(\chi(f_i(x))-\varepsilon_{d-1})\\&=\sum_{x\in GF(q)}\prod_{i=1}^{m}(\chi(f_i(x))^{d-1}+\chi(f_i(x))^{d-2}+\dots+\chi(f_i(x))+1).\end{aligned}$$

As N denotes the number of 'solutions', H is roughly $d^m N$ (because the product $(\chi(f_i(x))-\varepsilon_1)(\chi(f_i(x))-\varepsilon_2)\dots(\chi(f_i(x))-\varepsilon_{d-1})$ is zero if $\chi(f_i(x))\neq 1$ or 0; it is ± 1 if $f_i(x)=0$ and it is as big as d iff $\chi(f_i(x))=1$). An 'error term' comes from the zeros of the polynomials:

$$|H-d^m N|\leq d^{m-1}\sum_{i=1}^{m}\deg(f_i).$$

Let's examine H:

$$H=q+\sum_{x\in GF(q)}\sum_{j=1}^{m}\sum_{1\leq i_1<\ldots<i_j\leq m}\sum_{1\leq s_1,\ldots,s_j\leq d-1}\chi(f_{i_1}(x)^{s_1}f_{i_2}(x)^{s_2}\dots f_{i_j}(x)^{s_j}).$$

The second term (which is a real integer in fact, but it is not important for us now) has absolute value less than

$$|H-q|\leq\sum_{j=1}^{m}\sum_{1\leq i_1<\ldots<i_j\leq m}\sum_{1\leq s_1,\ldots,s_j\leq d-1}\left(\sum_{k=1}^{j}\deg(f_{i_k})s_k-1\right)\sqrt{q}$$

by Weil. But this is equal to

$$\begin{aligned}
&\sqrt{q}\sum_{j=1}^{m}\sum_{1\leq i_1<\ldots<i_j\leq m}\sum_{k=1}^{j}\deg(f_{i_k})(d-1)^{j-1}\sum_{l=1}^{d-1}l-\sqrt{q}\sum_{j=1}^{m}\binom{m}{j}(d-1)^j\\
=\;&\frac{d(d-1)}{2}\sqrt{q}\sum_{j=1}^{m}(d-1)^{j-1}\binom{m-1}{j-1}\sum_{i=1}^{m}\deg(f_i)-\sqrt{q}(d^m-1)\\
=\;&\frac{d(d-1)}{2}d^{m-1}\sqrt{q}\sum_{i=1}^{m}\deg(f_i)-\sqrt{q}(d^m-1).
\end{aligned}$$

Now, using the assumption

$$d^{m-1}\sum_{i=1}^{m}\deg(f_i)<\frac{q+\sqrt{q}(d^m-1)}{\frac{d(d-1)}{2}\sqrt{q}+1},$$

we have

$$\frac{d(d-1)}{2}d^{m-1}\sqrt{q}\sum_{i=1}^{m}\deg(f_i)-\sqrt{q}(d^m-1)+d^{m-1}\sum_{i=1}^{m}\deg(f_i)<q,$$

so $N>0$ and the existence of x_0 is proved. For the inequality we can divide the left hand side by d^m to get

$$|N-\frac{q}{d^m}|\leq\left(\frac{d-1}{2}\sqrt{q}+\frac{1}{d}\right)\sum_{i=1}^{m}\deg(f_i)-\sqrt{q}\left(1-\frac{1}{d^m}\right).$$

∎

References

[1] L. Babai, A. Gál and A. Wigderson, Superpolynomial lower bounds for monotone span programs, *Combinatorica*, to appear.

[2] Lidl and Niederreiter, *Finite fields*, Encyclopedy of Mathematics **20**, Addison-Wesley, Reading, 1983.

[3] T. Szőnyi, On the number of directions determined by a set of points in an affine Galois plane, *J. Comb. Theory A* **74** (1996), 141-146.

[4] T. Szőnyi, Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992), 227-235.

Technical University Budapest
Pázmány P. sétany 1/d, Budapest, Hungary H-1117
email : sziklai@cs.bme.hu