1. Introduction

Let $\mathbb{Z}_2^n$ denote the $n$-dimensional affine space over $\mathbb{Z}_2$. A multiset $S = \{x_1, \ldots, x_s\}$ is called a \textit{mod $p$ transversal} of $\mathbb{Z}_2^n$ if any hyperplane $H \subset \mathbb{Z}_2^n$ which does not contain 0 satisfies $|\{i : x_i \in H\}| \not\equiv 0 \pmod{p}$.

For a prime $p > 2$, let $f(p, n)$ denote the minimal cardinality (counting multiplicities) of such a mod-$p$ transversal.

Our interest in these quantities stems from a problems on Boolean circuit complexity which is described in section 4. The purpose of this note is to prove

\textbf{Theorem 1.} $e^{-1}(p-1)\frac{n}{p-1} - (p-1) \leq f(p, n) \leq (p-1)\left\lfloor \frac{n}{p-1} \right\rfloor - (p-1)$.

The lower bound is proved in section 2, using a Fourier transform approach. In section 3, we prove a version of the uncertainty principle (Theorem 2) which may be used to obtain a defect form of Theorem 1. It follows, for instance, that if $|S| = 2^{o(n/(p-1))}$, then $|S \cap H| \equiv 0 \pmod{p}$ for at least $2^{n(1-o(1))}$ hyperplanes $H$.

To show the upper bound of Theorem 1, we first note that since $f(p, n) \leq f(p, m)$ whenever $n \leq m$, it suffices to show that $f(p, (p-1)t) \leq (p-1)2^t - (p-1)$. To this end we partition $\{1, \ldots, (p-1)t\}$ into $p-1$ sets $I_1, \ldots, I_{p-1}$ of size $t$, and define $V_i = \{x \in \mathbb{Z}_2^n \setminus \{0\} : x_j = 0 \ \forall j \notin I_i\}$. It is clear that for any hyperplane $H$ not containing 0, $|H \cap V_i|$ is either 0 or $2^{t-1}$, and that the latter holds for at least one $i$. This implies that $S = \bigcup_{i=1}^{p-1} V_i$ is a mod $p$ transversal, and hence $f(p, n) \leq |S| = (p-1)(2^t - 1)$.

\textbf{AMS subject classification (1980):} 05, 68

Supported in part by AFOSR 0271. First author supported by NSF and a Sloan Research Fellowship.
As far as we know this upper bound may be sharp when $p - 1 | n$.

2. Mod $p$ transversals and the Fourier transform

Let $G$ be a finite abelian group and $K$ a field containing a primitive $m$-th root of 1, where $m = m(G)$ is the exponent of $G$ (i.e. the l.c.m. of the orders of the elements of $G$). A character of $G$ is a homomorphism $G \to K^\times$. The characters under pointwise multiplication form a group $\hat{G}$ which is isomorphic to $G$. The Fourier transform of a function $f : G \to K$ is the function $\hat{f} : \hat{G} \to K$ defined by

$$\hat{f}(\chi) = \sum_{x \in G} \chi(-x)f(x).$$

The convolution of two functions $f, g : G \to \mathbb{R}$ is given by

$$f \ast g(x) = \sum_{y \in G} f(y)g(x - y),$$

and its Fourier transform satisfies $\hat{f} \ast \hat{g}(x) = \hat{f}(x) \cdot \hat{g}(x)$. The unit element with respect to convolution is $u(x) = \delta_{0,x}$. We abbreviate $f \ast \cdots \ast f$ ($k$ factors) by $f^{\ast k}$, and for $A \subseteq G$ set $kA = \{a_1 + \cdots + a_k : a_i \in A\}$.

For the rest of this section we take $G = \mathbb{Z}_2^n$ and $K = \mathbb{Z}_p$. The Fourier transform of a function $f : \mathbb{Z}_2^n \to \mathbb{Z}_p$ is $\hat{f}(x) = \sum_{y \in \mathbb{Z}_2^n} f(y)(-1)^{y \cdot x}$ (where $x \cdot y$ denotes the standard inner product on $\mathbb{Z}_2^n$).

We turn now to the proof of the lower bound. Suppose $S = \{x_1, \ldots, x_s\}$ is a mod $p$ transversal of $\mathbb{Z}_2^n$, and for convenience let $0 \in S$. Let $f(x)$ denote the indicator function of $S$, and if $x \neq 0$ denote by $H_x$ the hyperplane $\{y : y \cdot x = 1\}$.

Set $g = su - f$. Then $\hat{g}(0) = 0$, and for each $x \neq 0$

$$\hat{g}(x) = s - \sum_{i=1}^{s} (-1)^{x_i \cdot x}$$

$$= \sum_{i=1}^{s} [1 - (-1)^{x_i \cdot x}]$$

$$= 2|\{i : 1 \leq i \leq s, \ x_i \in H_x\}|$$

$$\neq 0 \quad \text{(in $\mathbb{Z}_p$)}.$$

Letting $h = g^{(p-1)}$ we have $\hat{h}(x) = \hat{g}(x)^{p-1} = 1 - u$.

Thus $h(x) = 2^{-n}\hat{h}(x) = u(x) - 2^{-n}$, and in particular $\text{supp}(h) \supseteq \mathbb{Z}_2^n \setminus \{0\}$.

On the other hand,

$$\text{supp } h = \text{supp}(su - f)^{(p-1)} \subseteq (p - 1)\text{supp}(su - f) = (p - 1)|S|$$

(note $0 \in S$). Thus $(p - 1)S = \mathbb{Z}_2^n$, and so finally

$$s \geq e^{-1}(p - 1)^{p-1} - (p - 2)$$

follows from

$$2^n = |(p - 1)S| \leq |\{(a_1, \cdots, a_s) : a_i \geq 0, \ \sum a_i = p - 1\}| = \binom{p + s - 2}{p - 1}.$$
3. An uncertainty inequality for finite abelian groups

We shall need the following inequality which in the case \( K = \mathbb{C} \) is a well-known consequence of the uncertainty principle (e.g. [4]).

**Theorem 2.** If \( f : G \to K \) is not identically 0, then

\[
|\text{supp } f| |\text{supp } \hat{f}| \geq G.
\]

**Proof.** We argue by induction on the number of direct summands in \( G \). Assume first that \( G = \mathbb{Z}_m \), so that \( \hat{f}(k) = \sum_{\ell=0}^{m-1} f(\ell)\zeta^{-\ell k} \) where \( \zeta \) is some (fixed) primitive \( m \)-th root of 1. If \( t = |\text{supp } f| \), then there exists a cyclic interval \( \{a + 1, \ldots, a + \lfloor m/t \rfloor - 1\} \subset \mathbb{Z}_m \), which is disjoint from \( \text{supp } f \). Let \( b = a + \lfloor m/t \rfloor \), and consider the polynomial

\[
F(x) = \sum_{\ell=0}^{m-1} f(\ell + b)x^\ell \in K[x].
\]

We have

\[
F(\zeta^k) = \sum_{\ell=0}^{m-1} f(\ell + b)\zeta^{\ell k} = \zeta^{-kb} \sum_{\ell=0}^{m-1} f(\ell + b)\zeta^{(\ell + b)k} = \zeta^{-kb} \hat{f}(-k).
\]

On the other hand, \( f(a + i) = 0 \) for \( 1 \leq i \leq \lfloor m/t \rfloor - 1 \) implies \( \deg F \leq m - \lfloor m/t \rfloor \), whence \( F \) has at most \( m - \lfloor m/t \rfloor \) roots in \( K \), and in particular \( F(\zeta^k) \neq 0 \) for at least \( \lfloor m/t \rfloor \) values of \( k \). Thus \( |\text{supp } \hat{f}| \geq \lfloor m/t \rfloor \).

For the induction step, suppose that the theorem holds for \( G_1 \) and \( G_2 \), and let \( 0 \neq f : G_1 \oplus G_2 \to K \). For \( y \in G_2 \) define \( f_y : G_1 \to K \) by \( f_y(x) = f(x, y) \), and for \( x \in G_1 \) define \( F_x : G_2 \to K \) by \( F_x(y) = \hat{f}_y(x) \). For \( (\chi, \eta) \in \hat{G}_1 \oplus \hat{G}_2 \cong G_1 \oplus G_2 \) we have

\[
\hat{f}(\chi, \eta) = \sum_{x \in G_1} \sum_{y \in G_2} \chi(-x)\eta(-y)f(x, y) = \sum_{y \in G_2} \eta(-y)\hat{f}_y(\chi) = \hat{F}_x(\eta).
\]

So if \( F_x \neq 0 \), then by induction

\[
|\{ \eta \in \hat{G}_2 : \hat{f}(\chi, \eta) \neq 0 \}| = |\text{supp } \hat{F}_x| \geq \frac{|G_2|}{|\text{supp } \hat{F}_x|} \geq \frac{|G_2|}{|\{ z : f_z \neq 0 \}|}.
\]
Therefore, for any fixed $y \in G_2$

$$|\text{supp } \hat{f}| \geq \frac{|\text{supp } \hat{f}_y| \cdot |G_2|}{|\{z : f_z \neq 0\}|}.$$ 

Summing over all $y$, and using induction, we obtain

$$|\text{supp } f| |\text{supp } \hat{f}| = \sum_{\{y : f_y \neq 0\}} |\text{supp } f_y| \cdot |\text{supp } \hat{f}| 
\geq \sum_{\{y : f_y \neq 0\}} \frac{|\text{supp } f_y| \cdot |\text{supp } \hat{f}_y|} {|\{z : f_z \neq 0\}|} |G_2| 
\geq |G_1| \cdot |G_2|.$$ 

Theorem 2 easily implies the following quantitative version of Theorem 1.

**Corollary 3.** If $S \subset T^n_2$, $|S| = O\left(2^{(1-c)n} \frac{n}{p-1}\right)$, then $|H_x \cap S| \equiv 0 \pmod{p}$ for $\Omega(2^n)$ values of $\chi$.

**Proof.** With the notation of section 2, it is clear that $|H_x \cap S| \equiv 0 \pmod{p}$ iff $\hat{g}(x) = 0$ iff $(u - g^{*(p-1)})(x) \neq 0$. Hence

$$|\{x : |H_x \cap S| \equiv 0 \pmod{p}\}| = |\text{supp } (u - g^{*(p-1)})(x)| 
\geq \frac{2^n}{|\text{supp } (u - g^{*(p-1)})|} \geq \frac{2^n}{1 + (1 + s)^{p-1}} = \Omega(2^n).$$

4. Something like motivation

We assume some familiarity with Boolean (logical) circuits. (See e.g. [2]. Our circuits allow negated variables as inputs and place no restriction on fanin (=number of wires entering a gate).) For $m \in \mathbb{N}$ a $mod_m$-gate in a circuit is a gate which outputs 1 iff the mod $m$ sum of its inputs is 1 (0 otherwise). More generally an $m$-gate is any gate whose output depends only on the mod $m$ sum of its inputs. It is not hard to see that any $m$ gate may be (finitely) simulated by $mod_m$-gates.

For $p$ a prime power, a beautiful theorem of Smolensky [5] (following work of Razborov [3]) places a limits on the computational power of constant depth circuits which use $\land$, $\lor$- and $mod_m$-gates. In particular, such a circuit which computes the MAJORITY function of $n$ variables (i.e. $\text{MAJ}(x_1, \ldots, x_n) = 1$ iff $\sum x_i \geq n/2$) has $\exp(\Omega(n^{1/2d}))$ gates (where the implied constant depends on $p$). It has been conjectured by Barrington [1] that a similar result (at least with a superpolynomial lower bound) should hold for general $m$, but at this time essentially nothing is known for any $m$ not a prime power. This led us to consider the more restricted question of the power of constant depth circuits which use only $m$-gates, e.g.
Question. How large must a depth $d$ circuit be if it computes $\bigvee_{i=1}^{n} x_i$ using only $m$-gates?

It is not hard to see that if $m$ is a prime power then $\bigvee x_i$ cannot be computed at all. (For $m$ prime such a circuit computes a bounded degree polynomial in $\mathbb{Z}_m[x_1, \ldots, x_n]$, while $\bigvee x_i$ is a polynomial of degree $n$; the assertion for prime powers follows (see [5D]).)

It is thus a little surprising that if $m$ is not a prime power, there are depth 2 circuits using only $m$-gates which compute $\bigvee x_i$ (so also bounded depth circuits computing $\bigvee x_i$ and using only mod$_m$-gates). We show this for $m = 2p$. The general case is similar (although to maintain the depth at 2, rather than 3, we must allow multiple wires from an input to a gate at level 1). Let, then, $m = 2p$, and let $S = \{y_1, \ldots, y_s\}$ be a mod $p$ transversal of $\mathbb{Z}_2^n$, with $y_i = \{y_{i1}, \ldots, y_{in}\}$. For $i = 1, \ldots, s$ let $G_i$ be the mod$_2$-gate with input set $\{x_j : y_{ij} = 1\}$, and let $G$ be the $p$-gate with input set $\{G_1, \ldots, G_s\}$ which outputs 0 iff the inputs sum to 0 mod $p$.

(Note an $\ell$-gate is an $m$-gate if $\ell | m$.) It is easy to see that $G$ computes $\bigvee_{i=1}^{n} x_i$.

Thus the most one can hope for here is that computing $\bigvee x_i$ in depth $d$ with $m$-gates requires $\exp(\Omega(n^{f(d,m)}))$ gates for some $f(d,m) > 0$. In light of the above construction, our theorem is a (very) small step in this direction, but we are unable to go much further at this time.

Added in proof: Ravi Boppana has pointed out to us that a result equivalent to Theorem 1 (strictly speaking, only for $p = 3$) is proved in D. A. Barrington, Width 3 permutation branching programs, Technical Memorandum TM–291 (Dec. 1985), MIT Laboratory for CS, while a more general result for any two primes is given in D. A. Mix Barrington, H. Straubing and D. Thérien, Non-uniform automata over groups, Manuscript, August 1988.

References


Roy Meshulam

Center for Operations Research
Rutgers University
New Brunswick, NJ 08903
U.S.A.

Current address:
Department of Mathematics,
Technion,
Haifa 32000
Israel

Jeff Kahn

Department of Mathematics and
Center for Operations Research
Rutgers University
New Brunswick, NJ 08903
U.S.A.