Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 341 (2005) 279–282
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory

Bounds on an exponential sum arising in Boolean circuit complexity

Frederic Green [a], Amitabha Roy [b], Howard Straubing [b]

[a] *Department of Mathematics and Computer Science, Clark University, Worcester, MA 01610, USA*
[b] *Computer Science Department, Boston College, Chestnut Hill, MA 02467, USA*

Received 2 June 2005; accepted 4 July 2005

Available online 19 August 2005

Presented by Jean Bourgain

Abstract

We study exponential sums of the form $S = 2^{-n}\sum_{x\in\{0,1\}^n} e_m(h(x))e_q(p(x))$, where $m, q \in \mathbf{Z}^+$ are relatively prime, p is a polynomial with coefficients in $\mathbf{Z}_q$, and $h(x) = a(x_1 + \cdots + x_n)$ for some $1 \leqslant a < m$. We prove an upper bound of the form $2^{-\Omega(n)}$ on $|S|$. This generalizes a result of J. Bourgain, who establishes this bound in the case where q is odd. This bound has consequences in Boolean circuit complexity. ***To cite this article: F. Green et al., C. R. Acad. Sci. Paris, Ser. I 341 (2005).***

Résumé

Bornes sur une somme exponentielle liée à la complexité des circuits booléens. On étudie les sommes exponentielles de la forme $S = 2^{-n}\sum_{x\in\{0,1\}^n} e_m(h(x))e_q(p(x))$, où m, q sont des entiers premiers entre eux, p est un polynôme à coefficients dans $\mathbf{Z}_q$ et $h(x) = a(x_1 + \cdots + x_n)$, avec $1 \leqslant a < m$. On démontre que $|S| < 2^{-\Omega(n)}$. Ceci généralise un résultat de J. Bourgain, qui établit cette borne dans le cas où q est impair. Ce théorème a des conséquences dans l'étude de la complexité des circuits booléens. ***Pour citer cet article : F. Green et al., C. R. Acad. Sci. Paris, Ser. I 341 (2005).***

Version française abrégée

Soient $m, a, q \in \mathbf{Z}^+$ avec $1 \leqslant a < m$ et soit $p(x) = p(x_1, \ldots, x_n)$ un polynôme de degré d sur $\mathbf{Z}_q$. Nous étudions la somme exponentielle S (voir l'Éq. (1)). Bourgain, dans [2], énonce le théorème suivant :

Théorème 0.1. *Soit* $(m, q) = 1$. *Il existe* $0 < \mu_d < 1$ (*dépendant de* m, q, *et* d) *tel que*

$$|S| < \mu_d^n$$

E-mail addresses: fgreen@black.clarku.edu (F. Green), aroy@cs.bc.edu (A. Roy), straubin@cs.bc.edu (H. Straubing).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2005.07.011

pour tout $n > 0$. *De plus, pour tout* $0 < \epsilon < 1$, *il existe* $c > 0$ (*dépendant de* q) *tel que*

$$(\mu_{c \log n})^n < 2^{-n^\epsilon}$$

pour tout n *suffisamment grand.*

Cependant, la preuve de ce théorème dans [2] utilise une transformation de S en une somme exponentielle sur $\{-1, 1\}^n$, par le moyen de la substitution $x_i \mapsto \frac{1}{2}(1 - y_i)$, ce qui ne donne le résultat que dans le cas où q est impair. Ici nous modifions le raisonnement de [2] afin d'éviter cette substitution. Nous obtenons ainsi une démonstration valable pour tous les entiers m, q avec $(m, q) = 1$.

Le problème de borner la somme S a son origine en l'informatique théorique : Une borne supérieure de la forme 2^{-n^ϵ}, comme celle énoncée dans le Théorème 0.1, entraîne une borne supérieure 2^{n^ϵ} pour la taille minimum d'un circuit booléen, ayant une forme particulière, qui détermine si le nombre de 1 dans une suite binaire de longueur n est divisible par m. Les conséquences du Théorème 0.1 pour la complexité des circuits booléens, remarquées brièvement dans [2], sont exposées en détail par Alon et Beigel [1] et par Green [4].

1. Statement of the main result

Let $p(x) = p(x_1, \ldots, x_n)$ be a polynomial of degree d with coefficients in $\mathbf{Z}_q$. Let $m, q > 1$ and $1 \leqslant a < m$. We consider the exponential sum

$$S = 2^{-n} \sum_{x \in \{0,1\}^n} \left\{ e_m\left(a \sum_{i=1}^{n} x_i \right) e_q\big(p(x)\big) \right\}, \tag{1}$$

where $e_r(x)$ denotes $\exp(2\pi i x/r)$. We will show:

Theorem 1.1. *Let* $\gcd(m, q) = 1$. *There exists* $0 < \mu_d < 1$ (*depending on* m, q *and* d) *such that*

$$|S| < \mu_d^n$$

for all $n > 0$. *Moreover, for all* $0 < \epsilon < 1$, *there exists* $c > 0$ (*depending on* q) *such that*

$$(\mu_{c \log n})^n < 2^{-n^\epsilon}$$

for all sufficiently large n.

In other words, $|S|$ is exponentially small in n for each fixed d, and almost exponentially small even if d is allowed to grow as fast as $c \log n$.

Theorem 1.1 was stated by Bourgain in [2]. However, the proof given there replaces S by an exponential sum over $\{-1, 1\}^n$ via the change of variables $x_i \mapsto \frac{1}{2}(1 - y_i)$, which requires q to be odd. In the present note we modify the argument of [2] so as to avoid this change of variables, and thereby obtain a proof valid for all relatively prime pairs (m, q).

The problem of finding such exponentially small bounds on S originates in Computer Science, in the area of circuit complexity. The bounds proved here imply that circuits consisting of a majority gate at the output, mod q gates at the intermediate level, and AND gates of fan-in $c \log n$ at the inputs, must have size 2^{n^ϵ} in order to determine if the number of 1's in an n-bit input is divisible by m. Consequences of Theorem 1.1 for Boolean circuits are touched on briefly in [2], and discussed at length in Alon and Beigel [1] and in Green [4].

2. Proof of Theorem 1.1

The proof is by induction on the degree d of p. If $d=1$, then $p(x)=c_0+c_1x_1+\cdots+c_nx_n$, so

$$S=2^{-n}e_q(c_0)\prod_{i=1}^{n}\left(\sum_{x_i=0}^{1}e_m(ax_i)e_q(c_ix_i)\right)=e_q(c_0)\prod_{i=1}^{n}\frac{1}{2}\left[e_{qm}(aq+c_im)+1\right].$$

Since $\gcd(m,q)=1$, and $1\leqslant a<m$, we have $e_{qm}(aq+c_im)\neq 1$ and thus $|S|<(\mu_1)^n$, where $\mu_1=\frac{1}{2}|1+e_{qm}(1)|<1$.

Suppose now that $d>1$. We have

$$S^q=2^{-nq}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\left\{e_m\left(a\sum_{\substack{1\leqslant j\leqslant q\\1\leqslant i\leqslant n}}x_i^j\right)e_q\left(\sum_{j=1}^{q}p(x^j)\right)\right\}.$$

For $x,u\in\{0,1\}^n$, we denote by $x\oplus u$ the componentwise mod 2 sum of the bit vectors x and u. The map $x\mapsto x\oplus u$ is a permutation of $\{0,1\}^n$, so by averaging over all $u\in\{0,1\}^n$ we obtain

$$S^q=2^{-nq-n}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\sum_{u\in\{0,1\}^n}\left\{e_m\left(a\sum_{\substack{1\leqslant j\leqslant q\\1\leqslant i\leqslant n}}(x^j\oplus u)_i\right)e_q\left(\sum_{j=1}^{q}p(x^j\oplus u)\right)\right\}.$$

To each q-tuple $(x^1,\ldots,x^q)$ of n-dimensional bit vectors we assign the set $I=I(x^1,\ldots,x^q)$ of indices $i\in\{1,\ldots,n\}$ for which $x_i^1=\cdots=x_i^q=0$. We view a vector $u\in\{0,1\}^n$ as being composed of its projections $v\in\{0,1\}^{\bar I}$ and $w\in\{0,1\}^I$, and accordingly rewrite the preceding equation as

$$S^q=2^{-nq-n}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\sum_{v\in\{0,1\}^{\bar I}}\sum_{w\in\{0,1\}^I}\left\{e_m\left(a\sum_{\substack{1\leqslant j\leqslant q\\1\leqslant i\leqslant n}}(x^j\oplus u)_i\right)e_q\left(\sum_{j=1}^{q}p(x^j\oplus u)\right)\right\}.$$

Let us analyze the two factors appearing within the summation over $\{0,1\}^I$. Each expression of the form $(x^j\oplus u)_i$ occurring within these factors has the value w_i if $i\in I$, and is just some constant bit value (depending on the x^j and v, but independent of w) if $i\notin I$. Thus

$$e_m\left(a\sum_{\substack{1\leqslant j\leqslant q\\1\leqslant i\leqslant n}}(x^j\oplus u)_i\right)=\alpha\cdot e_m\left(aq\sum_{i\in I}w_i\right),$$

for some $\alpha\in\mathbf{C}$ of norm 1 not depending on w. Further, when $p(x^j\oplus u)$ is considered as a polynomial in the w_i, all terms of degree d that arise are independent of j. Thus all these terms cancel when the sum $\sum_{j=1}^{q}p(x^j\oplus u)$ is reduced modulo q. As a result we have

$$S^q=2^{-nq-n}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\sum_{v\in\{0,1\}^{\bar I}}\alpha\sum_{w\in\{0,1\}^I}\left\{e_m\left(aq\sum_{i\in I}w_i\right)e_q\left(p'(w)\right)\right\},$$

where p' is a polynomial of degree $d-1$ in $|I|$ variables that depends on the x^j and v. Since $\gcd(m,q)=1$, aq is not divisible by m, and so the inner summation over $\{0,1\}^I$ is an exponential sum of the form (1). We can thus apply the inductive hypothesis to obtain

$$|S|^q\leqslant 2^{-nq-n}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\sum_{v\in\{0,1\}^{\bar I}}2^{|I|}\mu_{d-1}^{|I|}=2^{-nq}\sum_{x^1,\ldots,x^q\in\{0,1\}^n}\mu_{d-1}^{|I|},$$

for some $0 < \mu_{d-1} < 1$.

Let $r \geqslant 0$. The number of q-tuples $(x^1, \ldots, x^q)$ for which $|I| = r$ is seen by a simple counting argument to be $\binom{n}{r}(2^q - 1)^{n-r}$. We thus have

$$|S|^q \leqslant 2^{-nq} \sum_{r=0}^{n} \binom{n}{r} (2^q - 1)^{n-r} \mu_{d-1}^r = 2^{-nq}(2^q - 1 + \mu_{d-1})^n,$$

so that

$$|S| \leqslant \left\{ \left(1 + \frac{\mu_{d-1} - 1}{2^q}\right)^{1/q} \right\}^n.$$

The first claim in Theorem 1.1 now follows by setting

$$\mu_d = \left(1 + \frac{\mu_{d-1} - 1}{2^q}\right)^{1/q}.$$

To prove the second claim in the theorem, we note that $(1-\gamma)^{1/q} < 1 - \gamma/q$ for all γ between 0 and 1, and thus

$$\mu_d < 1 - \frac{1 - \mu_{d-1}}{q2^q},$$

so that

$$1 - \mu_d > \frac{1 - \mu_1}{(q2^q)^d} = \frac{\beta}{(q2^q)^d},$$

where $0 < \beta < 1$ depends only on m and q. Thus

$$|S| \leqslant (\mu_d)^n < \left(1 - \frac{\beta}{(q2^q)^d}\right)^n.$$

Let $0 < \delta < 1$ and let $d = \delta \log n$, where the logarithm is taken to base $q2^q$. Then the right-hand side of the last inequality is $((1 - \beta/n^\delta)^{n^\delta})^{n^{1-\delta}}$, which is approximately $\exp(-\beta n^{1-\delta})$, and in any case smaller than $2^{-\beta n^{1-\delta}}$ for sufficiently large n. The second claim in Theorem 1.1 follows upon choosing $\delta < 1 - \epsilon$.

An open question of considerable interest in computational complexity is whether the degree bound in the second part of Theorem 1.1 can be extended to degrees up to $\log^k n$ where $k > 1$. (See the discussion in Green [4].) We also pose the related question of the optimal value for μ_d for fixed m, d, q. This is known only in the case where $m = d = 2$ and $q = 3$ [4]. Dueñez, et al. [3] investigate conjectured optimum values for $m = d = 2$ and all odd q, and prove these are optimal in some special cases.

Acknowledgements

We thank J. Bourgain for sending us his manuscript. The work of F. Green was supported in part by the National Security Agency (NSA) and Advanced Research and Development Agency (ARDA) under Army Research Office (ARO) contract number DAAD 19-02-1-0058.

References

[1] N. Alon, R. Beigel, Lower bounds for approximation by low-degree polynomials over Z_n, in: Annual IEEE Conference on Computational Complexity, vol. 16, 2001.
[2] J. Bourgain, Estimation of certain exponential sums arising in complexity theory, C. R. Acad. Sci. Paris, Ser. I 340 (2005) 627–631.
[3] E. Dueñez, S. Miller, A. Roy, H. Straubing, Incomplete quadratic exponential sums in several variables, J. Number Theory, in press.
[4] F. Green, The correlation between parity and quadratic polynomials mod 3, J. Comput. System Sci. 69 (1) (2004) 28–44.