BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(78), 2015, Pages 21–26
ISSN 1024–7696

Lower bound on product of binomial coefficients

Roman B. Popovych

Abstract. We give a lower bound on a product of binomial coefficients, connected with primality proving or construction of high multiplicative order elements in finite fields.

Mathematics subject classification: 05E40, 11T30.
Keywords and phrases: Product of binomial coefficients, primality proving, certificate, finite field, multiplicative order, lower bound.

1 Introduction and Preliminaries

Let m be a positive integer. The problem of finding such integers d_-, d $(0 \leq d_- \leq d < m)$ that the product of binomial coefficients

$$C(d_-, d) = \binom{m}{d_-}\binom{d}{d_-}\binom{2m - d_- - d - 1}{m - d - 1} \tag{1}$$

is large, appears in the following two cases.

1. AKS primality proving algorithm optimization.

Efficient primality tests (determining whether a given number is prime or composite) are needed in applications: a number of cryptographic protocols use big prime numbers.

In 2002 M. Agrawal, N. Kayal and N. Saxena [1] presented a deterministic polynomial time algorithm AKS that determines whether an input number n is prime or composite. It was proved [3] that AKS algorithm runs in $(\log n)^{7.5+o(1)}$ time. Significantly modified versions of AKS [3, 4] are also known with $(\log n)^{4+o(1)}$ running time. The algorithm in [3] uses a notion of certificate for an integer n. It is proved that if we have found the certificate for an integer, then this integer is a power of a prime. Then it is easy to decide if the integer is prime. During the certificate finding an essential point is to verify an inequality, for which it is necessary to calculate an expression of the form (1). We choose numbers d_-, d to construct the certificate.

2. Construction of high multiplicative order elements for finite field extensions.

The problem of constructing efficiently a primitive element for a given finite field is notoriously difficult in the computational theory of finite fields. That is why one considers less restrictive question: to find an element with high multiplicative order [8, 9]. It is sufficient in this case to obtain a lower bound on the order. High order elements are needed in several applications. Such applications include but are

not limited to cryptography, coding theory, pseudorandom number generation and combinatorics. The problem is considered both for general and special finite fields.

General extensions are considered in [7,13]. For special finite fields, it is possible to construct elements which can be proved to have much higher orders. Extensions connected with a notion of Gauss period are considered in [2,10]. Extensions based on Kummer polynomials are considered in [5,6,11].

F_q denotes finite field with q elements. According to [6, Lemma 2.1] we have the following lemma for extensions on a base of Kummer polynomials.

Lemma 1. *Let q be a prime power. Let m be a positive divisor of $q-1$. Let x^m-a ($a\in F_q^*$) be an irreducible polynomial in F_q and θ be one of its roots in the extension $F_{q^m}=F_q[x]/(x^m-a)$. Then for any $b\in F_q$ the element $\theta+b$ has the multiplicative order at least $D=\max\limits_{0\le d_-\le d<m} C(d_-,d)$.*

One can see that the product of the form (1) is present in Lemma 1. Therefore, the problem of product (1) maximization is important. It is shown in [3] that approximately for $d\approx m/2$ and $d_-\approx 0,2928m$ we have $C(d_-,d)\approx 5,8284^m$. Note that the value $5,8284^m$ is not a lower bound on D, but only some approximate value. Indeed, consider the following numerical examples.

For $m=37$, maximum D is achieved at $d_-=10, d=17$ and is equal to $D=C(10,17)\approx 2,81\cdot 10^{25}$. We do not compute precise integer value of D, because we only need to compare it with $(5,8284)^{37}=2,12\cdot 10^{28}$. For $m=511$, we have $D=C(149,254)\approx 4,17\cdot 10^{386}$. At the same time, $(5,8284)^{511}=1,57\cdot 10^{391}$.

From the point of view of applications (in particular, cryptography) an exact theoretical lower bound on D is desired. We give in the paper such explicit lower bound on maximum of the product (1) of binomial coefficients. In particular, bounds on binomial coefficients from [12] are used. The following inequality for binomial coefficients has been obtained in [12, Theorem 2.8, inequality (2.12)].

Lemma 2. *If r,s,t are integers with the conditions $s>r\ge 1$ and $t\ge 2$, then*

$$\binom{st}{rt} > (1/\sqrt{2\pi})\cdot e^{r-1/(8t)}\cdot t^{-1/2}\frac{s^{s(t-1)+1}}{(s-r)^{(s-r)(t-1)-r+1}\cdot r^{rt+1/2}}. \tag{2}$$

For $r=1$ we have the following corollary from inequality (2) [12, Corollary 2.9, inequality (2.13)].

Corollary 1. *For $s>1$ and $t\ge 2$ the following inequality holds:*

$$\binom{st}{t} > (1/\sqrt{2\pi})\cdot e^{1-1/(8t)}\cdot t^{-1/2}\frac{s^{s(t-1)+1}}{(s-1)^{(s-1)(t-1)}}. \tag{3}$$

Lemma 3. *The following equalities are true for binomial coefficients:*

$$\binom{u}{v}=\frac{u}{u-v}\binom{u-1}{v}, \tag{4}$$

$$\binom{u}{v}=\frac{u}{v}\binom{u-1}{v-1}. \tag{5}$$

Proof. To prove (4) note that $\binom{u}{v} = \frac{(u-v+1)\cdot\ldots\cdot u}{1\cdot 2\cdot\ldots\cdot v}$ and $\binom{u-1}{v} = \frac{(u-v)\cdot\ldots\cdot(u-1)}{1\cdot 2\cdot\ldots\cdot v}$. The observation that $\binom{u-1}{v-1} = \frac{(u-v+1)\cdot\ldots\cdot(u-1)}{1\cdot 2\cdot\ldots\cdot(v-1)}$ allows to prove (5). □

2 Main result

We give below in Theorem a lower bound on the maximum D of the product (1) of binomial coefficients. The proof of the theorem uses inequalities (2) and (3) from respectively Lemma 2 and Corollary 1.

Theorem 1. *Put $h = 4 \cdot 5^{5/4}/3^{3/2}$. For $m \geq 8$ the following lower bound holds:*

$$D > \frac{h^m}{30m^{3/2}}. \tag{6}$$

Proof. Take $k = m \bmod 4$, $d_- = (m-k)/4$, $d = (m-k)/2$. Show first that for $k \in \{0,1,2,3\}$

$$\binom{m}{d_-} = \binom{m}{(m-k)/4} > \beta(k)\binom{m-k}{(m-k)/4}, \tag{7}$$

where $\beta(0) = 1$, $\beta(1) = \frac{32}{25}$, $\beta(2) = \frac{16\cdot 14}{13\cdot 11}$, $\beta(3) = \frac{32\cdot\ 28\cdot 24}{27\cdot 23\cdot 19}$.

$\beta(0) = 1$ is clear. For $k = 1$, apply (4) to the left side of (7):

$$\binom{m}{(m-1)/4} = \frac{4m}{3m+1}\binom{m-1}{(m-1)/4}.$$

Since, for $m \geq 8$, the inequality $\frac{4m}{3m+1} \geq \frac{32}{25}$ holds, we have the above-mentioned $\beta(1)$. For $k = 2$, apply (4) subsequently 2 times:

$$\binom{m}{(m-2)/4} = \frac{4m}{3m+2}\binom{m-1}{(m-2)/4}, \binom{m-1}{(m-2)/4} = \frac{4(m-1)}{3(m-1)+1}\binom{m-2}{(m-2)/4}.$$

As, for $m \geq 8$, the conditions $\frac{4m}{3m+2} \geq \frac{16}{13}$, $\frac{4(m-1)}{3(m-1)+1} \geq 14/11$ are true, we have the foresaid $\beta(2)$. For $k = 3$, apply (4) subsequently 3 times:

$$\binom{m}{(m-3)/4} = \frac{4m}{3m+3}\binom{m-1}{(m-3)/4}, \binom{m-1}{(m-3)/4} = \frac{4(m-1)}{3(m-1)+2}\binom{m-2}{(m-3)/4},$$

$$\binom{m-2}{(m-3)/4} = \frac{4(m-2)}{3(m-2)+1}\binom{m-3}{(m-3)/4}.$$

Since, for $m \geq 8$, the inequalities $\frac{4m}{3m+3} \geq \frac{32}{27}$, $\frac{4(m-1)}{3(m-1)+2} \geq \frac{28}{23}$ and $\frac{4(m-2)}{3(m-2)+1} \geq \frac{24}{19}$ hold, we obtain the aforementioned $\beta(3)$.

Show now that

$$\binom{2m-d_--d-1}{m-d-1} = \binom{2m-3(m-k)/4-1}{m-2(m-k)/4-1} > \delta(k)\binom{5(m-k)/4}{2(m-k)/4}, \tag{8}$$

where $\delta(0)=\frac{1}{3}$, $\delta(1)=\frac{39}{25}$, $\delta(2)=\frac{21\cdot19\cdot17}{8\cdot13\cdot11}$, $\delta(3)=\frac{5\cdot41\cdot37\cdot33\cdot29}{2\cdot14\cdot27\cdot23\cdot19}$.

For $k=0$, apply (5) to the left side of (8):

$$\binom{5m/4-1}{2m/4-1}=\frac{2m/4-1}{5m/4-1}\binom{5m/4}{2m/4}.$$

As, for $m\geq 8$, the condition $\frac{2m/4-1}{5m/4-1}\geq\frac{3}{9}$ is true, we have $\delta(0)=\frac{1}{3}$. For $k=1$, apply the equality (4):

$$\binom{5(m-1)/4+1}{2(m-1)/4}=\frac{5(m-1)/4+1}{3(m-1)/4+1}\binom{5(m-1)/4}{2(m-1)/4}.$$

Since, for $m\geq 8$, the inequality $\frac{5(m-1)/4+1}{3(m-1)/4+1}\geq\frac{39}{25}$ holds, we have the aforesaid $\delta(1)$. For $k=2$, first apply (5):

$$\binom{5(m-2)/4+3}{2(m-2)/4+1}=\frac{5(m-2)/4+3}{2(m-2)/4+1}\binom{5(m-2)/4+2}{2(m-2)/4}.$$

Then apply (4) subsequently 2 times:

$$\binom{5(m-2)/4+2}{2(m-2)/4}=\frac{5(m-2)/4+2}{3(m-2)/4+2}\cdot\frac{5(m-2)/4+1}{3(m-2)/4+1}\binom{5(m-2)/4}{2(m-2)/4}.$$

For $m\geq 8$, since $\frac{5(m-2)/4+3}{2(m-2)/4+1}\geq\frac{21}{8}$, $\frac{5(m-2)/4+2}{3(m-2)/4+2}\geq\frac{19}{13}$ and $\frac{5(m-2)/4+1}{3(m-2)/4+1}\geq\frac{17}{11}$ are true, we obtain the foregoing $\delta(2)$. For $k=3$, first apply (5) 2 times:

$$\binom{5(m-3)/4+5}{2(m-3)/4+2}=\frac{5(m-3)/4+5}{2(m-3)/4+2}\cdot\frac{5(m-3)/4+4}{2(m-3)/4+1}\binom{5(m-3)/4+3}{2(m-3)/4}.$$

Then apply (4) subsequently 3 times:

$$\binom{5(m-3)/4+3}{2(m-3)/4}=\frac{5(m-3)/4+3}{3(m-3)/4+3}\cdot\frac{5(m-3)/4+2}{3(m-3)/4+2}\cdot\frac{5(m-3)/4+1}{3(m-3)/4+1}\binom{5(m-3)/4}{2(m-3)/4}.$$

For $m\geq 8$, since $\frac{5(m-3)/4+5}{2(m-3)/4+2}\geq\frac{5}{2}$, $\frac{5(m-3)/4+4}{2(m-3)/4+1}\geq\frac{41}{14}$, $\frac{5(m-3)/4+3}{3(m-3)/4+3}\geq\frac{37}{27}$, $\frac{5(m-3)/4+2}{3(m-3)/4+2}\geq\frac{33}{23}$ and $\frac{5(m-3)/4+1}{3(m-3)/4+1}\geq\frac{29}{19}$ hold, we have the forementioned $\delta(3)$.

Combining (7) and (8), we obtain that for $k\in\{0,1,2,3\}$ and $n=m-k$ the following inequality holds

$$D>\beta(k)\delta(k)\binom{n}{n/4}\binom{n/2}{n/4}\binom{5n/4}{2n/4}. \tag{9}$$

Now we give, using inequalities (2) or (3), lower bounds on each binomial coefficient on the right side of (9). Applying the inequality (2) to the first coefficient on the right side of (9) (in this case $t=n/4$, $s=4$), we have:

$$\binom{n}{n/4} > (1/\sqrt{2\pi}) \cdot e^{1-1/(2n)} (n/4)^{-1/2} \frac{4^{n-3}}{3^{3n/4-3}}. \tag{10}$$

Note, that $t \geq 2$ must hold, that is $m - k \geq 8$, and if $k = 0$, then $m \geq 8$. Applying the inequality (2) to the second coefficient (in this case $t = n/4$, $s = 2$), we have:

$$\binom{n/2}{n/4} > (1/\sqrt{2\pi}) \cdot e^{1-1/(2n)} (n/4)^{-1/2} 2^{n/2-1}. \tag{11}$$

Applying the inequality (3) to the third coefficient (in this case $t = n/4$, $s = 5$, $r = 2$), we have:

$$\binom{5n/4}{2n/4} > \frac{1}{\sqrt{2\pi}} \cdot e^{2-1/(2n)} (n/4)^{-1/2} \frac{5^{5n/4-4}}{2^{n/2-4} \cdot 3^{3n/4+1/2}}. \tag{12}$$

Substituting the inequalities (10), (11), (12) in the inequality (9), and taking into account that $\frac{1}{e^{3/(2(m-k))}} \geq \frac{1}{e^{3/(2(m-3))}}$, $1 < e^{3/(2(m-3))} < 1,35$ for $m \geq 8$, $\frac{1}{(m-k)^{3/2}} \geq \frac{1}{m^{3/2}}$, we obtain the bound

$$D > \frac{3^7 \cdot e^4}{10^5 \cdot \pi^{3/2} \cdot 1,35} \cdot \frac{\beta(k)\delta(k)}{h^k} \cdot \frac{h^m}{m^{3/2}}. \tag{13}$$

Since $\frac{3^7 \cdot e^4}{10^5 \cdot \pi^{3/2} \cdot 1,35} > 0,1588$, minimal value for $\frac{\beta(k)\delta(k)}{h^k}$ is at $k = 3$ and equals to 0,21, the last inequality is transformed into the bound (6). □

Obtained lower bound (6) on the product (1) of binomial coefficients is exact theoretical bound and comparable with the corresponding value from [3]. Taking into account in (6) that $5,7556 < 4 \cdot 5^{5/4}/3^{3/2} < 5,7557$, we have the following corollary.

Corollary 2. *For $m \geq 8$ the following inequality holds: $D > \frac{5,7556^m}{30m^{3/2}}$.*

Clearly for big enough m the main contribution on the right side of the last inequality is given by the term $(5,7556)^m$.

Remark that our result is a lower bound on D for $m \geq 8$ with constant 5,7556. If allow m to be bigger, say $m \geq 32$, then one obtains similar lower bound with constant 5,8230. To achieve this, choose in the proof of the theorem $d_- = m/4 + m/32$, $d = m/2$. For $m \geq 1024$, taking $d_- = m/4 + m/32 + m/128 + m/512 + m/1024$, $d = m/2$, one can obtain a bound with constant 5,8284.

References

[1] Agrawal M., Kayal N., Saxena N. *PRIMES is in P.* Ann. of Math., 2004, **160**, No. 2, 781–793.

[2] Ahmadi O., Shparlinski I. E., Voloch J. F. *Multiplicative order of Gauss periods.* Int. J. Number Theory, 2010, **6**, No. 4, 877–882.

[3] Bernstein D. *Proving primality in essentially quartic random time.* Math. Comp., 2007, **76**, No. 257, 391–403.

[4] Berrizbeitia P. *Sharpening Primes is in P for a large family of numbers.* Math. Comp., 2005, **74**, No. 252, 2043–2059.

[5] Burkhart J. F. et al. *Finite field elements of high order arising from modular curves.* Des. Codes Cryptogr., 2009, **51**, No. 3, 301–314.

[6] Cheng Q. *On the construction of finite field elements of large order.* Finite Fields Appl., 2005, **11**, No. 3, 358–366.

[7] Gao S. *Elements of provable high orders in finite fields.* Proc. Amer. Math. Soc., 1999, **107**, No. 6, 1615–1623.

[8] Lidl R., Niederreiter H. *Finite Fields.* Cambridge University Press, 1997.

[9] Mullen G. L., Panario D. *Handbook of finite fields.* CRC Press, 2013.

[10] Popovych R. *Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$.* Finite Fields Appl., 2012, **18**, No. 4, 700–710.

[11] Popovych R. *Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$.* Finite Fields Appl., 2013, **19**, No. 1, 86–92.

[12] Stanica P. *Good lower and upper bounds on binomial coefficients.* J. Inequal. Pure Appl. Math., 2001, **2**, No. 3, art. 30.

[13] Voloch J. F. *Elements of high order on finite fields from elliptic cures.* Bull. Austral. Math. Soc., 2010, **81**, No. 3, 425–429.

Roman B. Popovych
Lviv Polytechnic National University
Bandery Str.,12, Lviv, 79013
Ukraine

E-mail: *rombp07@gmail.com*

Received December 13, 2013
Revised July 27, 2015