# On additive complexity of a sequence of matrices * 

Igor S. Sergeev ${ }^{\dagger}$

## 1 Introduction

The present paper deals with the complexity of computation of a sequence of Boolean matrices via universal commutative additive circuits, i.e. circuits of binary additions over the group $(\mathbb{Z},+$ ) (an additive circuit implementing a matrix over $(\mathbb{Z},+)$, implements the same matrix over any commutative semigroup $(S,+)$.) Basic notions of circuit and complexity see in [3, [5].

Denote the complexity of a matrix $A$ over $(\mathbb{Z},+)$ as $L(A)$. Consider a sequence of $n \times n$-matrices $A_{n}$ with zeros on the leading diagonal and ones in other positions. It is known that $L\left(A_{n}\right)=3 n-6$, see e.g. [2].

In [4] it was proposed a sequence of matrices $B_{p, q, n}$ more general than $A_{n}$ and the question of complexity of the sequence was investigated. Matrix $B_{p, q, n}$ has $C_{n}^{q}$ rows and $C_{n}^{p}$ columns. Rows are indexed by $q$-element subsets of $[1 . . n]$; columns are indexed by $p$-element subsets of $[1 . . n]$ (here $[k . . l]$ stands for $\{k, k+1, \ldots, l\})$. A matrix entry at the intersection of $Q$-th row and $P$-th column is 1 if $Q \cap P=\emptyset$ and 0 otherwise.

Consider some simple examples of $B_{p, q, n}$. If $n<p+q$ then $B_{p, q, n}$ is zero matrix. Evidently, $B_{1,1, n}=A_{n}$. By the symmetry of definition $B_{p, q, n}=$ $B_{q, p, n}^{T}$. Matrices $B_{p, 0, n}$ and $B_{0, q, n}$ are all-ones row and column respectively. So, $L\left(B_{p, 0, n}\right)=C_{n}^{p}-1, L\left(B_{0, q, n}\right)=0$.

Note that by the transposition principle (see e.g. [3]) complexity of matrices $B_{p, q, n}$ and $B_{q, p, n}$ satisfies the identity

$$
L\left(B_{q, p, n}\right)=L\left(B_{p, q, n}\right)+C_{n}^{q}-C_{n}^{p} .
$$

[^0]It was shown in [4] that $L\left(B_{p, q, n}\right)=O\left(\left(n^{p}+n^{q}\right) \log n\right)$. We prove better bound

$$
L\left(B_{p, q, n}\right) \leq\left(\alpha^{p}-1\right) C_{n}^{q}+\alpha^{q} C_{n}^{p}
$$

where $\alpha=\frac{3+\sqrt{5}}{2}$. This bound is linear (and consequently tight up to a constant factor) for a constant $p$ and $q \leq 0.65 n$.

The following lower bound

$$
L\left(B_{p, q, n}\right) \geq(q-p+1) \sum_{k=0}^{p} C_{n}^{k}-2^{p+q}
$$

valid for $1 \leq p \leq q$ and $n>p+q$, shows that the complexity of $B_{p, q, n}$ is generally non-linear. For instance, one can try $p$ and $q$ of type $\frac{n}{2}-\Theta(\sqrt{n})$ to obtain $L\left(B_{p, q, n}\right)=\Omega(N \log N)$, where $N=C_{n}^{p}+C_{n}^{q}$.

## 2 Algorithm

Let us introduce some notation. Let $\left\langle p, q, S_{0}, S\right\rangle$ denote a set of sums $y_{Q}=$ $\sum_{P \subset S \backslash Q,|P|=p} x_{S_{0} \cup P}$, where $Q \subset S,|Q|=q$. Thus, $\langle p, q, \emptyset,[1 . . n]\rangle$ is a result of multiplication of the matrix $B_{p, q, n}$ by the vector of variables $x_{P}, P \subset[1 . . n]$, $|P|=p$.

Let $\langle p, q, \emptyset,[1 . . n-1]\rangle$ is already computed (with complexity $L\left(B_{p, q, n-1}\right)$ ). We are to compute $\langle p, q, \emptyset,[1 . . n]\rangle$. The computation consists of three parts.

1. Computation of $y_{Q},\{1, n\} \cap Q=\emptyset$.
1.1. Connect each input $x_{\{1\} \cup S}$ of a circuit computing $\langle p, q, \emptyset,[1 . . n-1]\rangle$ with the following precomputed sum

$$
\begin{gathered}
x_{\{1\} \cup S}+x_{\{n\} \cup S}, \quad \text { if } 2 \notin S, \\
\sum_{T \subset([1 . k] \cup\{n\}),|T|=k} x_{T \cup S^{\prime}}, \quad \text { if } S=[2 . . k] \sqcup S^{\prime} \text { and }(k+1) \notin S, \quad k \leq p-1 .
\end{gathered}
$$

Note that in the sums above each variable $x_{\{n\} \cup S}$ occurs exactly once. Thus, these sums can be computed with complexity $C_{n-1}^{p-1}$.
1.2. Consider functioning of outputs of the transformed circuit. Take an output implementing a sum $y_{Q} \in\langle p, q, \emptyset,[1 . . n-1]\rangle$ in the original circuit. If $1 \in Q$, then functioning of the output remained intact after transformation since $y_{Q}$ depends on inputs which haven't changed. If $[1 . . k] \cap Q=\emptyset$ and $(k+1) \in Q, 1 \leq k \leq p-1$, then the output in the transformed circuit computes a sum

$$
\begin{equation*}
\sum_{P \cap Q=\emptyset,|P|=p,([1 . . k] \cup\{n\}) \not \subset P} x_{P} . \tag{1}
\end{equation*}
$$

To obtain a sum $y_{Q} \in\langle p, q, \emptyset,[1 . . n]\rangle$ one has to add summands $x_{P},([1 . . k] \cup$ $\{n\}) \subset P$, to the sum (1). At last, if $[1 . . p] \cap Q=\emptyset$, then the output correctly computes a sum $y_{Q} \in\langle p, q, \emptyset,[1 . . n]\rangle$ in the transformed circuit.
1.3. For any $k \in[1 . . p-1]$ compute

$$
\langle p-k-1, q-1,[1 . . k] \cup\{n\},[k+2 . . n-1]\rangle .
$$

These are all sums needed to complete sums (1) to obtain $\langle p, q, \emptyset,[1 . . n]\rangle$.
The complexity of the computations can be estimated as

$$
\sum_{k=2}^{p} L\left(B_{p-k, q-1, n-k-1}\right) .
$$

1.4. Add the sums computed on the step 1.3 to sums (1). Complexity of this addition is the number of sums (1), i.e. the number of $q$-element sets $Q \subset[2 . . n-1]$ such that $[2 . . p] \cap Q \neq \emptyset$. The latter number is $C_{n-2}^{q}-C_{n-p-1}^{q}$.
2. Computation of $y_{Q},|\{1, n\} \cap Q|=1$.
2.1. In the current circuit consider outputs implementing sums $y_{Q} \in$ $\langle p, q, \emptyset,[1 . . n-1]\rangle, 1 \in Q$ (this outputs implemented the same sums in the original circuit). Each such sum can be expanded to a sum $y_{Q} \in\langle p, q, \emptyset,[1 . . n]\rangle$, $1 \notin Q, n \in Q$ (alternatively, $1 \in Q, n \notin Q$ ), via addition of summands $x_{P}$, $1 \in P, P \subset[1 . . n-1]$ (respectively, $n \in P, P \subset[2 . . n]$ ).
2.2. Compute sets $\langle p-1, q-1,1,[2 . . n-1]\rangle$ and $\langle p-1, q-1, n,[2 . . n-1]\rangle$ with complexity $2 L\left(B_{p-1, q-1, n-2}\right)$.
2.3. Add the last computed sums to the sums $y_{Q} \in\langle p, q, \emptyset,[1 . . n-1]\rangle$, $1 \in Q$. It requires $2 C_{n-2}^{q-1}$ elementary additions.
3. Computation of $y_{Q},\{1, n\} \subset Q$.
3.1. Note that any $q$-element set $Q \subset[1 . . n],\{1, n\} \subset Q$, satisfies condition: $[1 . . k-1] \subset Q, n \in Q, k \notin Q$ for some $k \in[2 . . q]$.

Let $k \in[2 . . q]$. In the current circuit consider outputs implementing sums $y_{Q} \in\langle p, q, \emptyset,[1 . . n-1]\rangle,[1 . . k] \subset Q,(k+1) \notin Q$. (This set can be defined alternatively as $\langle p, q-k, \emptyset,[k+1 . . n-1]\rangle$.) Such sum can be expanded to a sum $y_{Q} \in\langle p, q, \emptyset,[1 . . n]\rangle,[1 . . k-1] \subset Q, n \in Q, k \notin Q$, via addition of appropriate summands $x_{P}, k \in P, P \subset[k . . n-1]$. The supplementing sums constitute the set $\langle p-1, q-k, k,[k+1 . . n-1]\rangle$.
3.2. For any $k \in[2 . . q]$ compute the set $\langle p-1, q-k, k,[k+1 . . n-1]\rangle$. It requires complexity

$$
\sum_{k=2}^{q} L\left(B_{p-1, q-k, n-k-1}\right) .
$$

3.3. Add the latter computed sums to the sums $y_{Q} \in\langle p, q, \emptyset,[1 . . n-1]\rangle$ according to the item 3.1. It requires $C_{n-2}^{q-2}$ elementary additions, by the number of results.

## 3 Upper bound

The argument of the previous section leads to inequality:

$$
\begin{align*}
& L\left(B_{p, q, n}\right) \leq L\left(B_{p, q, n-1}\right)+C_{n-1}^{p-1}+C_{n}^{q}-C_{n-p-1}^{q}+ \\
& \quad+\sum_{k=1}^{p} L\left(B_{p-k, q-1, n-k-1}\right)+\sum_{k=1}^{q} L\left(B_{p-1, q-k, n-k-1}\right), \tag{2}
\end{align*}
$$

due to identity $C_{n-2}^{q}+2 C_{n-2}^{q-1}+C_{n-2}^{q-2}=C_{n}^{q}$.
Theorem 1 Let $\alpha=\frac{3+\sqrt{5}}{2}$. Then

$$
L\left(B_{p, q, n}\right) \leq\left(\alpha^{p}-1\right) C_{n}^{q}+\alpha^{q} C_{n}^{p} .
$$

Proof. The statement of the theorem is evidently holds when $n=p+q$, or $p=0$, or $q=0$ (see introduction). Let us assume the validity of the statement for all triples of parameters $p^{\prime}, q^{\prime}, n^{\prime}$, where $p^{\prime} \leq p, q^{\prime} \leq q, n^{\prime}<n$ and consider the triple $p, q, n$.

Put the assumed upper bounds in the second member of (2). To make calculations easier use identities:

$$
\begin{gathered}
C_{n}^{q}-C_{n-p-1}^{q}=C_{n-1}^{q-1}+C_{n-2}^{q-1}+\ldots+C_{n-p-1}^{q-1} \leq(p+1) C_{n-1}^{q-1}, \\
C_{n}^{0}+C_{n+1}^{1}+\ldots C_{n+k}^{k}=C_{n+k+1}^{k} .
\end{gathered}
$$

The last identity allows to estimate sums in (2) as following:

$$
\begin{aligned}
\sum_{k=1}^{p} L\left(B_{p-k, q-1, n-k-1}\right) \leq \alpha^{q-1} \sum_{k=1}^{p} & C_{n-k-1}^{p-k}+C_{n-1}^{q-1}\left(\sum_{k=0}^{p-1} \alpha^{k}-p\right) \leq \\
& \leq \alpha^{q-1} C_{n-1}^{p-1}+\left(\frac{\alpha^{p}}{\alpha-1}-p-1\right) C_{n-1}^{q-1}
\end{aligned} \quad \begin{aligned}
& \sum_{k=1}^{q} L\left(B_{p-1, q-k, n-k-1}\right) \leq\left(\alpha^{p-1}-1\right) \sum_{k=1}^{q} C_{n-k-1}^{q-k}+C_{n-1}^{p-1} \sum_{k=0}^{q-1} \alpha^{k} \leq \\
& \leq\left(\alpha^{p-1}-1\right) C_{n-1}^{q-1}+\left(\frac{\alpha^{q}}{\alpha-1}-1\right) C_{n-1}^{p-1}
\end{aligned}
$$

Finally, taking into account $1+\frac{\alpha}{\alpha-1}=\alpha$, the second member of (21) is bounded by

$$
\left(\alpha^{p}-1\right) C_{n-1}^{q}+\alpha^{q} C_{n-1}^{p}+\left(\alpha^{p}-1\right) C_{n-1}^{q-1}+\alpha^{q} C_{n-1}^{p-1} \leq\left(\alpha^{p}-1\right) C_{n}^{q}+\alpha^{q} C_{n}^{p},
$$

q.e.d.

## 4 Lower bound

Lemma 1 If $n \geq p+q$, then matrix $B_{p, q, n}$ has full rank over $\mathbb{R}$.
Proof. By invariance of rank with respect to transposition it is sufficient to consider case $p \leq q$ (so, $C_{n}^{p} \leq C_{n}^{q}$ ).

We are to show that the rows of $B_{p, q, n}$ generate the space $\mathbb{R}^{C_{n}^{p}}$. To be precise, we will prove that any vector $(0, \ldots, 0,1,0 \ldots, 0)$ with 1 in position $P$ can be represented as a linear combination of rows of $B_{p, q, n}$.

Let $a_{0}, \ldots, a_{p} \in \mathbb{R}$. Consider such linear combination of rows, in which $Q$ th row occurs with the coefficient $a_{|P \cap Q|}$. Clearly, such combination produces a vector with coordinate in position $P^{\prime}$ depending only on $\left|P \cap P^{\prime}\right|$. Denote the value of this coordinate as $b_{\left|P \cap P^{\prime}\right|}$.

1. We are going to prove that a vector $\left(b_{0}, \ldots, b_{p}\right)^{T}$ is the product of a vector $\left(a_{p}, \ldots, a_{0}\right)^{T}$ and some constant upper triangular matrix $H$ with no zeros on the leading diagonal.
1.1. Firstly, check that $b_{i}$ depends on $a_{p-i}$ (hence, the leading diagonal of $H$ contains no zeros). Indeed, let $P^{\prime} \subset[1 . . n]$ and $\left|P \cap P^{\prime}\right|=i$. Consider a row indexed by $Q, Q \cap P=P \backslash P^{\prime}, Q \cap P^{\prime}=\emptyset$. Such row exists in view of inequality $n \geq p+q$. The row has 1 in position $P^{\prime}$ and it occurs in the linear combination with the coefficient $a_{p-i}$.
1.2. Analogous argument shows that $b_{i}$ does not depend on $a_{p-j}$ if $j<i$ (hence, all entries in $H$ below leading diagonal are zero). Indeed, for any $Q$, $|Q \cap P|=p-j$, one immediately concludes that $\left|Q \cap P^{\prime}\right| \geq i-j>0$. So the $Q$-th row has zero in position $P^{\prime}$.
2. Therefore, for any vector $\bar{b} \in \mathbb{R}^{p+1}$, in particular for the vector $(0, \ldots, 0,1)$ we are interested in, there exists a vector $\bar{a} \in \mathbb{R}^{p+1}$ such that $\bar{b}=H \bar{a}$. The vector $\bar{a}$ defines the required linear combination, q.e.d.

Lemma 2 Let $p \geq 1, q \geq 1, n>p+q$. Then

$$
L\left(B_{p, q, n}\right) \geq L\left(B_{p, q-1, n-1}\right)+L\left(B_{p-1, q, n-1}\right)+C_{n-1}^{\min \{p, q\}} .
$$

Proof. The proof of the lemma is similar to the proof of Th. 4 in [1]. Consider an arbitrary additive circuit $\Psi$ implementing $B_{p, q, n}$. Write $X_{0}=\left\{x_{P} \mid n \notin\right.$ $P\}, X_{1}=\left\{x_{P} \mid n \in P\right\}$.

1. Consider the subcircuit of $\Psi$ which does not depend on inputs $X_{0}$. Particularly, it implements the set $\langle p, q-1, \emptyset,[1 . . n-1]\rangle$ and consequently contains at least $L\left(B_{p, q-1, n-1}\right)$ gates.
2. Calculate the number of gates in $\Psi$ with both inputs depending on inputs from $X_{1}$. These gates together form a circuit derived from $\Psi$ by replacement of inputs from $X_{0}$ by zeros. In particular, this circuit computes
$\langle p-1, q, n,[1 . . n-1]\rangle$. Thus, the number of gates in question is at least $L\left(B_{p-1, q, n-1}\right)$.
3. Now, consider the gates of $\Psi$ with one input depending on $X_{1}$ and another input not depending on $X_{1}$. Denote as $Y$ a set of sums of variables in $X_{0}$ implemented by non-depending on $X_{1}$ inputs of the gates. Note that $|Y|$ is a lower bound for the number of the considered gates. It can be also seen that $Y$ generates the set $\langle p, q, \emptyset,[1 . . n-1]\rangle$ containing $X_{0}$-parts of sums implementing by $\Psi$ and depending on $X_{1}$. Thus, $|Y| \geq \operatorname{rk} B_{p, q, n-1}$. As follows from Lemma 1, rk $B_{p, q, n-1}=C_{n-1}^{\min \{p, q\}}$.

By putting estimates of items $1-3$ together one obtains the required inequality.
Theorem 2 Let $n>p+q$ and $p \leq q$. Then

$$
L\left(B_{p, q, n}\right) \geq(q-p+1) \sum_{k=0}^{p} C_{n}^{k}-2^{p+q} .
$$

Proof. The proof is by induction as in Th. 1. Put the cases $p=0$ and $p=q=1$ as a base of induction $\left(L\left(B_{1,1, n}\right) \geq n-3\right.$ evidently holds, see introduction).

1. If $p<q$ then by the Lemma 2 and induction hypothesis one has

$$
\begin{aligned}
& L\left(B_{p, q, n}\right) \geq C_{n-1}^{p}+(q-p) \sum_{k=0}^{p} C_{n-1}^{k}+(q-p+2) \sum_{k=0}^{p-1} C_{n-1}^{k}-2^{p+q}= \\
= & (q-p+1) \sum_{k=1}^{p}\left(C_{n-1}^{k}+C_{n-1}^{k-1}\right)+(q-p+1)-2^{p+q}=(q-p+1) \sum_{k=0}^{p} C_{n}^{k}-2^{p+q} .
\end{aligned}
$$

2. In the case $p=q$ use transposition property

$$
L\left(B_{p, p-1, n}\right)=L\left(B_{p-1, p, n}\right)+C_{n-1}^{p}-C_{n-1}^{p-1},
$$

to obtain

$$
\begin{aligned}
L\left(B_{p, p, n}\right) \geq 2 C_{n-1}^{p}-C_{n-1}^{p-1}+4 & \sum_{k=0}^{p-1} C_{n-1}^{k}-2^{2 p}> \\
& >C_{n-1}^{p}+2 \sum_{k=0}^{p-1} C_{n-1}^{k}-2^{2 p}=\sum_{k=0}^{p} C_{n}^{k}-2^{2 p}
\end{aligned}
$$

It completes the proof.
Remark. In fact, Lemma 2 allows to deduce slightly stronger inequality

$$
L\left(B_{p, q, n}\right) \geq C_{n}^{p}+\sum_{k=0}^{p}(p+q-2 k+1) C_{n}^{k}-2^{p+q+1}
$$

## References

[1] Boyar J., Find M. G. Cancellation-free circuits: an approach for proving superlinear lower bounds for linear Boolean operators. arXiv:1207.5321.
[2] Chashkin A. V. On the complexity of Boolean matrices, graphs and their corresponding Boolean functions. Diskretnaya matematika. 1994. 6(2), 43-73 (in Russian). [English translation in Discrete Math. and Appl. 1994. 4(3), 229-257.]
[3] Jukna S. Boolean function complexity. Berlin, Heidelberg: SpringerVerlag, 2012. 618 p.
[4] Kaski P., Koivisto M., Korhonen J. H. Fast monotone summation over disjoint sets. arXiv:1208.0554.
[5] Lupanov O. B. Asymptotic bounds for the complexity of control systems. Moscow: MSU, 1984. 138 p. (in Russian)


[^0]:    *Research supported in part by RFBR, grants 11-01-00508, 11-01-00792, and OMN RAS "Algebraic and combinatorial methods of mathematical cybernetics and information systems of new generation" program (project "Problems of optimal synthesis of control systems").
    ${ }^{\dagger} \mathrm{e}$-mail: isserg@gmail.com

