On additive complexity of a sequence of matrices *

Igor S. Sergeev[†]

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 $L(A_n) = 3n - 6$, 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 $n then <math>B_{p,q,n}$ 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, $L(B_{p,0,n}) = C_n^p - 1$, $L(B_{0,q,n}) = 0$.

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

$$L(B_{q,p,n}) = L(B_{p,q,n}) + C_n^q - C_n^p.$$

^{*}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").

[†]e-mail: isserg@gmail.com

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

$$L(B_{p,q,n}) \le (\alpha^p - 1)C_n^q + \alpha^q C_n^p,$$

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

The following lower bound

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

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 $L(B_{p,q,n}) = \Omega(N \log N)$, where $N = C_n^p + C_n^q$.

2 Algorithm

Let us introduce some notation. Let $\langle p, q, S_0, S \rangle$ denote a set of sums $y_Q = \sum_{P \subset S \setminus Q, |P|=p} x_{S_0 \cup P}$, 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 $L(B_{p,q,n-1})$). 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

$$x_{\{1\}\cup S} + x_{\{n\}\cup S}, \quad \text{if } 2 \notin S,$$

$$\sum_{T \subset ([1..k] \cup \{n\}), |T|=k} x_{T \cup S'}, \quad \text{if } S = [2..k] \sqcup S' \text{ and } (k+1) \notin S, \quad k \le p-1.$$

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

$$\sum_{P \cap Q = \emptyset, |P| = p, ([1..k] \cup \{n\}) \not \subset P} x_P.$$
(1)

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

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

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 (p-1, q-1, 1, [2..n-1]) and (p-1, q-1, n, [2..n-1]) with complexity $2L(B_{p-1,q-1,n-2})$.

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 $2C_{n-2}^{q-1}$ 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

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

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:

$$L(B_{p,q,n}) \leq L(B_{p,q,n-1}) + C_{n-1}^{p-1} + C_n^q - C_{n-p-1}^q + \sum_{k=1}^p L(B_{p-k,q-1,n-k-1}) + \sum_{k=1}^q L(B_{p-1,q-k,n-k-1}), \quad (2)$$

due to identity $C_{n-2}^q + 2C_{n-2}^{q-1} + C_{n-2}^{q-2} = C_n^q$.

Theorem 1 Let $\alpha = \frac{3+\sqrt{5}}{2}$. Then

$$L(B_{p,q,n}) \le (\alpha^p - 1)C_n^q + \alpha^q C_n^p.$$

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', q', n', where $p' \leq p, q' \leq q, n' < n$ and consider the triple p, q, n.

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

$$C_n^q - C_{n-p-1}^q = C_{n-1}^{q-1} + C_{n-2}^{q-1} + \ldots + C_{n-p-1}^{q-1} \le (p+1)C_{n-1}^{q-1},$$

$$C_n^0 + C_{n+1}^1 + \ldots + C_{n+k}^k = C_{n+k+1}^k.$$

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

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

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

Finally, taking into account $1 + \frac{\alpha}{\alpha - 1} = \alpha$, the second member of (2) is bounded by

$$(\alpha^p - 1)C_{n-1}^q + \alpha^q C_{n-1}^p + (\alpha^p - 1)C_{n-1}^{q-1} + \alpha^q C_{n-1}^{p-1} \le (\alpha^p - 1)C_n^q + \alpha^q C_n^p$$

q.e.d.

4 Lower bound

Lemma 1 If $n \ge p + q$, 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 Qth row occurs with the coefficient $a_{|P \cap Q|}$. Clearly, such combination produces a vector with coordinate in position P' depending only on $|P \cap P'|$. Denote the value of this coordinate as $b_{|P \cap P'|}$.

1. We are going to prove that a vector $(b_0, \ldots, b_p)^T$ is the product of a vector $(a_p, \ldots, a_0)^T$ 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 $P' \subset [1..n]$ and $|P \cap P'| = i$. Consider a row indexed by $Q, Q \cap P = P \setminus P', Q \cap P' = \emptyset$. Such row exists in view of inequality $n \ge p + q$. The row has 1 in position P' 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 $|Q \cap P'| \ge i - j > 0$. So the Q-th row has zero in position P'.

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 $p \ge 1$, $q \ge 1$, n > p + q. Then

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

Proof. The proof of the lemma is similar to the proof of Th. 4 in [1]. Consider an arbitrary additive circuit Ψ implementing $B_{p,q,n}$. Write $X_0 = \{x_P \mid n \notin P\}, X_1 = \{x_P \mid n \in P\}.$

1. Consider the subcircuit of Ψ 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 $L(B_{p,q-1,n-1})$ gates.

2. Calculate the number of gates in Ψ with both inputs depending on inputs from X_1 . These gates together form a circuit derived from Ψ 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 $L(B_{p-1,q,n-1})$.

3. Now, consider the gates of Ψ 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 Ψ and depending on X_1 . Thus, $|Y| \ge \operatorname{rk} B_{p,q,n-1}$. As follows from Lemma 1, $\operatorname{rk} B_{p,q,n-1} = C_{n-1}^{\min\{p,q\}}$.

By putting estimates of items 1-3 together one obtains the required inequality.

Theorem 2 Let n > p + q and $p \le q$. Then

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

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

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

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

2. In the case p = q use transposition property

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

to obtain

$$L(B_{p,p,n}) \ge 2C_{n-1}^p - C_{n-1}^{p-1} + 4\sum_{k=0}^{p-1} C_{n-1}^k - 2^{2p} >$$

> $C_{n-1}^p + 2\sum_{k=0}^{p-1} C_{n-1}^k - 2^{2p} = \sum_{k=0}^p C_n^k - 2^{2p}.$

It completes the proof.

Remark. In fact, Lemma 2 allows to deduce slightly stronger inequality

$$L(B_{p,q,n}) \ge C_n^p + \sum_{k=0}^p (p+q-2k+1)C_n^k - 2^{p+q+1}$$

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: Springer-Verlag, 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)