Implementation of linear maps with circulant matrices via modulo 2 rectifier circuits of bounded depth*

Igor S. Sergeev†

Abstract

In the present note we show that for any constant $k \in \mathbb{N}$ an arbitrary Boolean circulant matrix can be implemented via modulo 2 rectifier circuit of depth $2k-1$ and complexity $O\left(n^{1+1/k}\right)$, and also via circuit of depth $2k$ and complexity $O\left(n^{1+1/k}\log^{-1/k} n\right)$.

Recall that *rectifier* (m,n)*-circuit* is an oriented graph with n vertices labeled as inputs and m vertices labeled as outputs. *Modulo* 2 *rectifier circuit* implements a Boolean $m\times n$ matrix $A=(a_{i,j})$ iff for any i and j the number of oriented paths from j-th input to i-th output is congruent to $a_{i,j}$ modulo 2. Complexity of a circuit is the number of edges in it, circuit depth is the maximal length of an oriented path. See details in [3, 4].

$n \times n$ matrix $Z=(z_{i,j})$ is *circulant* iff for any i, j one has $z_{i,j}=z_{0,k}$, where $k=(j-i) \bmod n$.

Consider a linear map with Boolean circulant $n\times n$ matrix — it computes a cyclic (algebraic, over $GF(2)$) convolution with some constant vector A. Indeed, components of vector $C=(C_0,\ldots,C_{n-1})$ which is a convolution of vectors $A=(A_0,\ldots,A_{n-1})$ and $B=(B_0,\ldots,B_{n-1})$ satisfy formulae:

$$C_k = \sum_{i+j\equiv k \mod n} A_i B_j.$$

The following theorem allows to extend results [1, 2] on comparison of complexity of implementation of some circulant matrices via rectifier circuits and modulo 2 rectifier circuits to bounded depth circuits.

*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

Theorem 1. *For any $k \in \mathbb{N}$ an arbitrary Boolean circulant $n \times n$ matrix Z can be implemented via modulo 2 rectifier circuit:*

a) of depth $2k-1$ and complexity at most $f(2k-1)n^{1+1/k}$;

b) of depth $2k$ and complexity at most $f(2k)n\left(\frac{n}{\log n}\right)^{1/k}$.

The proof is by induction. For $k = 1$ we use a trivial depth-1 circuit of complexity $O(n^2)$ and a circuit of depth 2 and complexity $O(n^2/\log n)$ provided by O.B. Lupanov's method [4].

Now we prove an induction step from $k-1$ to k. We use the polynomial multiplication method due to A.L. Toom [6] together with . Schönhage's idea [5] allowing to extend the method to binary polynomials. The depth-d polynomial multiplication is reduced to several parallel depth-$(d-2)$ multiplications.

Split a vector of variables into q blocks of length n/q and interpret each block as a vector of coefficients of a polynomial from the ring

$$R = GF(2)[y]/(y^{2\cdot 3^s} + y^{3^s} + 1).$$

Parameter s satisfies condition $3^s \geq n/q$.

So, multiplication of binary polynomials of degree $n-1$ can be performed as a multiplication of polynomials of degree $n/q-1$ over R. The latter multiplication can be performed via DFT of order $3^m \geq 2q$ with primitive root $\zeta = y^{s+1-m} \in R$.

Next, we describe a circuit.

Its input is a polynomial $B(x) = \sum B_i x^i \in R[x]$ of degree $q-1$. A constant factor is denoted by $A(x) = \sum A_i x^i$. Output is the product $C(x) = A(x)B(x) = \sum C_i x^i$.

1. Compute $B(\zeta^0)$, ..., $B(\zeta^{3^m-1})$.
2. Compute $C(\zeta^i) = A(\zeta^i)B(\zeta^i)$ for all $i = 0, \dots, 3^m-1$.
3. Compute coefficients of $C(x)$.

We implement stages 1 and 3 via depth-1 circuits and stage 2 — via circuit of depth $d-2$. Next, we estimate the circuit complexity, denote it by $M(d,n)$.

1. Multiplication by a power of y in R has linear complexity. Hence, the value of polynomial $F(x)$ at the point y^p can be computed with linear complexity as well. Therefore, the complexity of stage 1 is $O(3^m 3^s q)$.

2. Every multiplication at the stage 2 is a multiplication of binary polynomials of degree $2\cdot 3^s - 1$ with a subsequent modulo reduction. Perform multiplication via circuit of depth $d-2$ and complexity $M(d-2, 2\cdot 3^s)$ provided by induction hypothesis. Reduction of a polynomial $g(y)$ (here, of degree $4\cdot 3^s - 1$) modulo $y^{2\cdot 3^s} + y^{3^s} + 1$ is performed via duplication of some

of its coefficients (that is, outputs of a preceding subcircuit) and identifying of some coefficients, since every coefficient of g is to be used at most twice. Henceforth, modulo reduction can be embedded into multiplication circuit with no depth increasing and with at most doubling of the circuit complexity. Thus, the total complexity of stage 2 is at most $2 \cdot 3^m M(d-2, 2 \cdot 3^s)$.

3. By the fundamental property of DFT, coefficients of $C(x)$ satisfy $C_i = C^*(\zeta^{-i})$, where polynomial $C^*(x)$ has coefficients $C(\zeta^i)$. Thus, the complexity of stage 3 is that of stage 1, $O(3^m 3^s q)$.

To transform the product of polynomials over R backward to the product of binary polynomials, one performs a substitution $x = y^{2 \cdot 3^s}$. The substitution preserves depth and complexity of the circuit.

The choice of parameters to obtain required complexity bounds is: $q = n^{1/k}$ for $d = 2k-1$ and $q = (n/\log n)^{1/k}$ for $d = 2k$; $3^s = \Theta(n/q)$, $3^m = \Theta(q)$.

(By construction, $f(k) = O(c^k)$ for some constant c.) $\square$

References

[1] Gashkov S. B., Sergeev I. S. On the complexity of linear Boolean operators with thin matrices. J. Applied and Industrial Math. 2011. **5**(2), 202–211.

[2] Grinchuk M. I., Sergeev I. S. Thin circulant matrices and lower bounds on the complexity of some Boolean operators. Diskretn. Anal. Issled. Oper. 2011. **18**(5), 38–53 (in Russian).

[3] Jukna S. Boolean function complexity. Advances and frontiers. Springer–Verlag, 2012.

[4] Lupanov O. B. On rectifier and switching-and-rectifier circuits. Dokl. Akad. Nauk SSSR. 1956. **111**(6), 1171–1174 (in Russian).

[5] Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2. Acta Inf. 1977. **7**, 395–398.

[6] Toom A. L. The complexity of a scheme of functional elements realizing the multiplication of integers. Soviet Math. Doklady. 1963. **4**, 714–716.