мы можем построить m схем, каждая из которых вычисляет φ_i: $G_i \times G_i \to G_i$ и требует количество времени $\tau_i = 2 + \left\rceil \log_{\left\lceil \frac{r+1}{2} \right\rceil} \frac{1}{\left\lceil \frac{r}{2} \right\rceil} \right\rceil \log_d |G_i| \left\lceil \right\rceil$ для вычисления этой функции. Так что вся схема может может вычислить свою функцию за время

$$\tau = \max_{1<=i<=m} \tau_i = 2 + \left\rceil \log_{\left\lceil \frac{r+1}{2} \right\rceil} \frac{1}{\left\lceil \frac{r}{2} \right\rceil} \right\rceil \log_d \alpha(G) \left\lceil \right\rceil .$$

(Идея доказатеьства здесь та же, что в [3].)

Сравнение теоремы 2 с теоремой 1 показывает, что с ростом r время, требующееся для вычисления φ: $G \times G \to G$, для конечной абелевой группы приближается к нижней оценке. Более точно, пусть $\tau_{\mathtt{act}}$ обозначает время, полученное в теореме 2, а $\tau_{\mathtt{min}}$ обозначает нижнюю оценку, полученную в теореме 1; тогда

$$\tau_{\text{act}} = 2 + \left\rceil \log_{\left\lceil \frac{r+1}{2} \right\rceil} \frac{1}{\left\lceil \frac{r}{2} \right\rceil} \right\rceil \log_d \alpha(G) \left\lceil \right\rceil \approx$$

$$\approx 2 + \log_{\left\lceil \frac{r+1}{2} \right\rceil} \frac{1}{\left\lceil \frac{r}{2} \right\rceil} \left\rceil \log_d \alpha(G) \right\lceil \approx$$

$$\approx 2 - \log_{\left\lceil \frac{r+1}{2} \right\rceil} \left\lceil \frac{r}{2} \right\rceil + \left\rceil \log_r \log_d \alpha(G) \right\lceil \log_{\left\lceil \frac{r+1}{2} \right\rceil} r.$$

Итак, для достаточно больших r, таких, что $\log_{\left\lceil \frac{r+1}{2} \right\rceil} \left\lceil \frac{r}{2} \right\rceil \approx 1$ и $\log_{\left\lceil \frac{r+1}{2} \right\rceil} r \approx 1$, мы получаем $\tau_{\text{act}} \approx \tau_{\text{min}} + 1$.

5. ОБСУЖДЕНИЕ

В разд. 3 мы видели, что нижняя оценка времени, требуемого для вычисления групповой операции, для конечной группы G зависит от логарифма логарифма порядка некоторой p-подгруппы группы G. В случае, когда G - абелева группа (и, в частности если G есть Z_μ, где групповой операцией является сложение по модолю μ), эта p-подгруппа представляет собой наибольшую циклическую подгруппу, порядок которой есть степень простого. В разд. 4 мы видели, что к этой нижней оценке можно приблизиться, если число входных линий логических элементов, используемых для построения схемы, увеличивается.

Эти результаты зависят от конкретного определения понятия «логическая схема C способна вычислить функцию φ».

В нашем определении мы потребовали, чтобы входы схемы были разделены на классы и каждый класс соответствовал одному аргументу вычисляемой функции. Это было сделано для того, чтобы функция φ действительно вычислялась схемой, а для этого входы должны нести информацию только об аргументах, но не о способе их комбинирования для получения результата. Читатель легко убедиться в том, что если бы мы заменили требование, наложенное на g_i в определении 3, требованием существования g_j': $I'_{c,\,j} \subset I_{c,\,j} \longrightarrow X_j$, то мы получили бы эквивалентное определение.

Требование существования функции h: $Y \to O_c$ эквивалентно требованию существования h': $O'_c \subset O_c \xrightarrow{1:1} Y$. Целью требования 1:1 для h' было устранить возможность того, чтобы выходы несли в точности ту же самую информацию, что и входы, и чтобы функция h' «действительно» выполняла вычисление. Разумеется, возможны и другие определения понятия вычисления, которые еще соответствуют нашим интуитивным представлениям. В [4] описана схема сложения, в которой требование, наложенное на h', ослаблено, а именно взамен потребовано, чтобы один и тот же код использовался как для кодирования каждого из слагаемых, так и для кодирования результата.

Другой чертой определения 3 является фиксированное время τ, через которое обследуется выход. Другой подход состоит в том, чтобы рассматривать время «установления» схем, которое, конечно, зависит от конкретных значений, принимаемых аргументами, и затем считать среднее время «установления» схемы временем вычисления (см. [5]). Предполагается, что это среднее время имеет тот же самый порядок, что и нижняя оценка, однако доказать это предположение нам не удалось.

Другое направление исследования состоит в рассмотрении обоих параметров — и времени вычисления и числа логических элементов, требующихся для построения схемы (см. [1]). Этот подход можно даже соединить с ослаблением допущения о том, что входы несут всю информацию об аргументах в момент времени $\tau=0$, разрешив подавать входы в схему «последовательно».

Благодарности. Автор благодарен М. О. Рабину за предложение задачи о времени вычисления сложения при ограничении, что компоненты имеют r входов, а также за постановку вопроса о том, может ли быть это время улучшено, если не пользоваться позиционным представлением чисел.