$Q = Q(y_1,\ldots,y_n)$ by $Q = Q(y_1,\ldots,y_n) = P(y_1+2,\ldots,y_n+2)-2$, and $T = \{(y_1,\ldots,y_n) \in \{1,-1\}^n : (y_1+2,\ldots,y_n+2) \in S\}$, where all additions are in $GF(3)$. Clearly $Q$ has degree at most $\sqrt{n}$ and $Q(y_1,,\ldots,y_n) = \prod_{i=1}^{n} y_i$ for all $(y_1,\ldots,y_n) \in T$. Let now $G = G(y_1,\ldots,y_n) : T \to GF(3)$ be an arbitrary function. Extend it in an arbitrary way to a function from $(GF(3))^n \to GF(3)$, and write this function as a polynomial in $n$ variables. [Trivially, any function from $(GF(3))^n \to GF(3)$ is a polynomial. This follows from the fact that it is a linear combination of functions of the form $\prod_{i=1}^{n}(y_i-\varepsilon_i)(y_i-\varepsilon_i-1)$, where $\varepsilon_i \in GF(3)$]. Replace each occurance of $y_i^2$ in this polynomial by 1 to obtain a multilinear polynomial $\tilde{G}$ which agrees with $G$ on $T$. Now replace each monomial $\prod_{i\in U} y_i$, where $|U| > \frac{n}{2}+\frac{\sqrt{n}}{2}$ by $\prod_{i\notin U} y_i \cdot Q(y_1,\ldots,y_n)$, and replace this new polynomial by a multilinear one, $\tilde{\tilde{G}}$, again by replacing each $y_i^2$ by 1. Since for $y_i \in \{\pm 1\}$, $\prod_{i\notin U} y_i \cdot \prod_{i=1}^{n} y_i = \prod_{i\in U} y_i$, $\tilde{\tilde{G}}$ is equal to $G$ on $T$ and its degree is at most $\frac{n}{2}+\frac{\sqrt{n}}{2}$. However, the number of possible $\tilde{\tilde{G}}$ is $3^{\sum_{i=0}^{\frac{n}{2}+\frac{\sqrt{n}}{2}}\binom{n}{i}} < 3^{0.88\cdot 2^n}$, whereas the number of possible $G$ is $3^{|T|} \geq 3^{0.9\cdot 2^n}$. This is impossible, and hence the assertion of the lemma holds. ■

**Corollary 11.3.3** *There is no circuit of depth $d$ and size $s \leq \frac{1}{10}2^{\frac{1}{2}}n^{1/2d}$ computing the parity of $x_1, x_2, \ldots, x_n$ using Not, And, Or and* $\mathrm{Mod}_3$ *gates.*

**Proof.** Suppose this is false and let $C$ be such a circuit. Put $\ell = \frac{1}{2}\cdot n^{1/2d}$. By Lemma 11.3.1 there is a polynomial $P = P(x_1,\ldots,x_n)$ over $GF(3)$, whose degree is at most $(2\ell)^d = \sqrt{n}$, which is equal to the parity of $x_1,\ldots,x_n$ on at least $2^n(1-\frac{s}{2^{\frac{1}{2}}n^{1/2d}}) \geq 0.9\cdot 2^n$ inputs. This contradicts Lemma 11.3.2, and hence completes the proof. ■

## 11.4 MONOTONE CIRCUITS

A Boolean function $f = f(x_1,\ldots,x_n)$ is *monotone* if $f(x_1,\ldots,x_n) = 1$ and $x_i \leq y_i$ imply $f(y_1,\ldots,y_n) = 1$. A *binary monotone circuit* is a binary circuit that contains only binary *And* and *Or* gates. It is easy to see that a function is monotone if and only if there is a binary montone circuit that computes it. The *monotone complexity* of a monotone function is the smallest size of a binary monotone circuit that computes it. Until 1985, the largest known lower bound for the monotone complexity of a monotone **NP**-function of $n$ variables was $4n$. This was considerably improved in the fundamental paper of Razborov (1985), where a bound of $n^{\Omega(\log n)}$ to the $\mathrm{Clique}_k$-function (which is 1 iff a given graph contains a clique of size $k$) is established. Shortly afterwards, Andreev (1985) used similar

methods to obtain an exponential lower bound to a somewhat unnatural **NP**-function. Alon and Boppana (1987) strengthened the combinatorial arguments of Razborov and proved an exponential lower bound for the monotone circuit complexity of the clique function. In this section we describe a special case of this bound by showing that there are no linear size monotone circuits that decide if a given graph contains a triangle. Although this result is much weaker than the ones stated above, it illustrates nicely all the probabilistic considerations in the more complicated proofs and avoids some of the combinatorial subtleties, whose detailed proofs can be found in the above mentioned papers.

Put $n = \binom{m}{2}$, and let $x_1, x_2, \ldots, x_n$ be $n$ Boolean variables representing the edges of a graph on the set of vertices $\{1, 2, \ldots, m\}$. Let $T = T(x_1, \ldots, x_n)$ be the monotone Boolean function whose value is 1 if the corresponding graph contains a triangle. Clearly, there is a binary monotone circuit of size $O(m^3)$ computing $T$. Thus, the following theorem is tight, up to a polylogarithmic factor.

**Theorem 11.4.1** *The monotone circuit complexity of $T$ is at least $\Omega(m^3/\log^4 m)$.*

Before we present the proof of this Theorem we introduce some notation and prove a simple lemma. For any Boolean function $f = f(x_1, \ldots, x_n)$ define $A(f) = \{(x_1, \ldots, x_n) \in \{0,1\}^n : f(x_1, \ldots, x_n) = 1\}$. Clearly $A(f \vee g) = A(f) \cup A(g)$ and $A(f \wedge g) = A(f) \cap A(g)$. Let $C$ be a monotone circuit of size $s$ computing the function $f = f(x_1, \ldots, x_n)$. Clearly, $C$ supplies a monotone straight-line program of length $s$ computing $f$, i.e., a sequence of functions $x_1, x_2, \ldots, x_n, f_1, \ldots, f_s$, where $f_s = f$ and each $f_i$, for $1 \leq i \leq s$, is either an *Or* or an *And* of two of the previous functions. By applying the operation $A$ we obtain a sequence $A(C)$ of subsets of $(0,1)^n$ : $A_{-n} = A_{x_n}, \ldots, A_{-1} = A_{x_1}, A_1, \ldots, A_s$ where $A_{x_i} = A(x_i)$, $A_s = A(f)$ and each $A_i$, for $1 \leq i \leq s$ is either a union or an intersection of two of the previous subsets. Let us replace the sequence $A(C)$ by an *approximating sequence* $M(C)$ : $M_{-n} = M_{x_n} = A_{x_n}, \ldots, M_{-1} = M_{x_1} = A_{x_1}, M_1, \ldots, M_s$ defined by replacing the union and intersection operations in $A(C)$ by the approximating operations $\sqcup$ and $\sqcap$, respectively. The exact definition of these two operations will be given later, in such a way that for all admissible $M$ and $L$ the inclusions

$$M \sqcup L \supseteq M \cup L \quad \text{and} \quad M \sqcap L \subseteq M \cap L \tag{11.9}$$

will hold. Thus $M_{x_i} = A_{x_i}$ for all $1 \leq i \leq n$, and if for some $1 \leq j \leq s$ we have $A_j = A_\ell \cup A_k$ then $M_j = M_\ell \sqcup M_k$, whereas if $A_j = A_\ell \cap A_k$ then $M_j = M_\ell \sqcap M_k$. In the former case put $\delta_\sqcup^j = M_j - (M_\ell \cup M_k)$ and $\delta_\sqcap^j = \phi$, and in the latter case put $\delta_\sqcap^j = (M_\ell \cap M_k) - M_j$ and $\delta_\sqcup^j = \phi$.

**Lemma 11.4.2** *For all members $M_i$ of $M(C)$,*

$$A_i - \left( \bigcup_{j \leq i} \delta_\sqcap^j \right) \subseteq M_i \subseteq A_i \cup \bigcup_{j \leq i} \delta_\sqcup^j . \tag{11.10}$$

**Proof.** We apply induction on $i$. For $i < 0$ $M_i = A_i$ and thus (11.10) holds. Assuming (11.10) holds for all $M_j$ with $j < i$ we prove it for $i$. If $A_i = A_\ell \cup A_k$,

then, by the induction hypothesis,

$$M_i = M_\ell \cup M_k \cup \delta^i_\sqcup \subseteq A_\ell \cup A_k \cup \bigcup_{j\le i} \delta^j_\sqcup = A_i \cup \bigcup_{j\le i} \delta^j_\sqcup$$

and

$$\begin{aligned} M_i &= M_\ell \sqcup M_k \supseteq M_\ell \cup M_k \supseteq \left(A_\ell - \left(\bigcup_{j\le \ell} \delta^j_\sqcap\right)\right) \cup \left(A_k - \left(\bigcup_{j\le k} \delta^j_\sqcap\right)\right) \\ &\supseteq A_i - \left(\bigcup_{j\le i} \delta^j_\sqcap\right), \end{aligned} \tag{11.11}$$

as needed. If $A_i = A_\ell \cap A_k$ the proof is similar. ■

Lemma 11.4.2 holds for any choice of the operations $\sqcup$ and $\sqcap$ which satisfies (11.9). In order to prove Theorem 11.4.1 we define these operations as follows. Put $r = 100 \log^2 m$. For any set $R$ of at most $r$ edges on $V = \{1, 2, \ldots, m\}$, let $\lceil R \rceil$ denote the set of all graphs on $V$ containing at least one edge of $R$. In particular $\lceil \phi \rceil$ is the empty set. We also let $\lceil * \rceil$ denote the set of all graphs. The elements of $M(C)$ will all have the form $\lceil R \rceil$ or $\lceil * \rceil$. Note that $A_{x_i} = M_{x_i}$ is simply the set $\lceil R \rceil$ where $R$ is a singleton containing the appropriate single edge. For two sets $R_1$ and $R_2$ of at most $r$ edges each, we define $\lceil R_1 \rceil \sqcap \lceil R_2 \rceil = \lceil R_1 \cap R_2 \rceil$, $\lceil R_1 \rceil \sqcap \lceil * \rceil = \lceil R_1 \rceil$ and $\lceil * \rceil \sqcap \lceil * \rceil = \lceil * \rceil$. Similarly, if $|R_1 \cup R_2| \le r$ we define $\lceil R_1 \rceil \sqcup \lceil R_2 \rceil = \lceil R_1 \cup R_2 \rceil$ whereas if $|R_1 \cup R_2| > r$ then $\lceil R_1 \rceil \sqcup \lceil R_2 \rceil = \lceil * \rceil$. Finally $\lceil * \rceil \sqcup \lceil R_1 \rceil = \lceil * \rceil \sqcup \lceil * \rceil = \lceil * \rceil$.

**Proof [theorem 11.4.1]** We now prove Theorem 11.4.1 by showing that there is no monotone circuit of size $s < \binom{m}{3}/2r^2$ computing the function $T$. Indeed, suppose this is false and let $C$ be such a circuit. Let $M(C) = M_{x_n}, \ldots, M_{x_1}, M_1, \ldots, M_s$ be an approximating sequence of length $s$ obtained from $C$ as described above. By Lemma 11.4.2,

$$A(T) - \left(\bigcup_{j\le s} \delta^j_\sqcap\right) \subseteq M_s \subseteq A(T) \cup \bigcup_{j\le s} \delta^j_\sqcup . \tag{11.12}$$

We consider two possible cases.

*Case 1* $M_s = \lceil R \rceil$, where $|R| \le r$.

Let us choose a random triangle $\Delta$ on $\{1, 2, \ldots, m\}$. Clearly

$$\Pr(\Delta \in M_s) \le \frac{r \cdot (m-2)}{\binom{m}{3}} < \frac{1}{2} .$$

Moreover, for each fixed $j$, $j \le s$,

$$\Pr(\Delta \in \delta^j_\sqcap) \le \frac{r^2}{\binom{m}{3}} .$$

This is because if $\delta_{\sqcap}^j \neq \phi$, then $\delta_{\sqcap}^j = (\lceil R_1 \rceil \cap \lceil R_2 \rceil) - \lceil R_1 \cap R_2 \rceil$ for some two sets of edges $R_1$, $R_2$, each of cardinality at most $r$. The only triangles in this difference are those containing an edge from $R_1$ and another edge from $R_2$ (and no edge of both). Since there are at most $r^2$ such triangles the last inequality follows. Since $s < \binom{m}{3}/2r^2$ the last two inequalities imply that $\Pr(\Delta \notin M_s \text{ and } \Delta \notin \bigcup_{j \leq s} \delta_{\sqcap}^j) > 0$ and thus there is such a triangle $\Delta$. Since this triangle belongs to $A(T)$ this contradicts (11.12), showing that Case 1 is impossible.

*Case 2* $M_s = \lceil * \rceil$.

Let $B$ be a random spanning complete bipartite graph on $V = \{1, 2, \ldots, m\}$ obtained by coloring each vertex in $V$ randomly and independently by 0 or 1 and taking all edges connecting vertices with distinct colors. Since $M_s$ is the set of all graphs, $B \in M_s$. Also $B \notin A(T)$, as it contains no triangle. We claim that for every fixed $j$, $j \leq s$,

$$\Pr(B \in \delta_{\sqcup}^j) \leq 2^{-\sqrt{r}/2} < \frac{1}{m^5} . \tag{11.13}$$

Indeed, if $\delta_{\sqcup}^j \neq \phi$, then $\delta_{\sqcup}^j = \lceil * \rceil - (\lceil R_1 \rceil \cup \lceil R_2 \rceil)$, where $|R_1 \cup R_2| > r$. Consider the graph whose set of edges is $R_1 \cup R_2$. Let $d$ be its maximum degree. By Vizing's theorem the set of its edges can be partitioned into at most $d + 1$ matchings. Thus either $d > \frac{\sqrt{r}}{2}$ or the size of the maximum matching in this graph is at least $\sqrt{r}/2$. It follows that our graph contains a set of $k = \sqrt{r}/2$ edges $e_1, \ldots, e_k$ which form either a star or a matching. In each of these two cases $\Pr(e_i \in B) = \frac{1}{2}$ and these events are mutually independent. Hence

$$\Pr(B \notin \lceil R_1 \rceil \cup \lceil R_2 \rceil) \leq 2^{-\sqrt{r}/2} ,$$

implying (11.13). Note that a similar estimate can be established without Vizing's theorem by observing that $B$ does not belong to $(\lceil R_1 \rceil \cup \lceil R_2 \rceil)$ if and only if the vertices in any connected component of the graph whose edges are $R_1 \cup R_2$ belong to the same color class of $B$.

Since $s < \binom{m}{3}/2r^2 < m^5$, inequality (11.13) implies that there is a bipartite $B$ such that $B \in M_s$, $B \notin A(T)$ and $B \notin \bigcup_{j \leq s} \delta_{\sqcup}^j$. This contradicts (11.12), shows that Case 2 is impossible and hence completes the proof of Theorem 11.4.1 ■