the particle thus resembles a random walk on the line where the particle
moves from the \( i \)-th position (\( 0 < i < n \)) to position \( i - 1 \) with probability
\( p_{i,i-1} \geq 1/2 \). This implies that

\[
t(i) \leq \frac{t(i - 1) + t(i + 1)}{2} + 1.
\]

Replace the obtained inequalities by equations

\[
\begin{align*}
x(0) &= 0, \\
x(i) &= \frac{x(i - 1) + x(i + 1)}{2} + 1, \\
x(n) &= x(n - 1) + 1.
\end{align*}
\]

This resolves to \( x(1) = 2n - 1 \), \( x(2) = 4n - 4 \) and in general \( x(i) = 2in - i^2 \). Therefore, \( t(i) \leq x(i) \leq x(n) = n^2 \), as desired.

By Markov’s inequality, a random variable can take a value \( 2 \) times larger
than its expectation with probability at most \( 1/2 \). Thus, the probability that
the particle will make more than \( 2 \cdot t(i) \) steps to reach position 0 from position
\( i \), is smaller than \( 1/2 \). Hence, with probability at least \( 1/2 \) the process will
terminate in at most \( 2n^2 \) steps, as claimed.

\( \Box \)

### 23.1.2 Schöning’s algorithm for 3-SAT

Can one design a similar algorithm also for 3-SAT? In the algorithm for
2-SAT above the randomness was only used to flip the bits—the initial as-
signment can be chosen arbitrarily: one could always start, say, with a fixed
assignment \((1, 1, \ldots, 1)\). But what if we choose this initial assignment at ran-
dom? If a formula is satisfiable, then we will “catch” a satisfying assignment
with probability at least \( 1/2 \). Thus, the probability that
the particle will make more than \( 2 \cdot t(i) \) steps to reach position 0 from position
\( i \), is smaller than \( 1/2 \). Hence, with probability at least \( 1/2 \) the process will
terminate in at most \( 2n^2 \) steps, as claimed.

For a satisfiable 3-CNF \( F \), let \( p(F) \) be the probability that Schöning’s
algorithm finds a satisfying assignment, and let \( p(n) = \min p(F) \) where
the minimum is over all satisfiable 3-CNFs in \( n \) variables. So, \( p(n) \) lower bounds
the success probability of the above algorithm.

It is clear that \( p(n) \geq (1/2)^n \): any fixed satisfying assignment \( a^* \) will be
“caught” in Step (1) with probability \( 2^{-n} \). It turns out that \( p(n) \) is much
23.1 The satisfiability problem

larger—it is at least about \( p = (3/4)^n \). Thus, the probability that after, say, \( t = 30(4/3)^n \) re-starts we will not have found a satisfying assignment is at most \( (1 - p)^t \leq e^{-pt} = e^{-30} \), an error probability with which everybody can live quite well.

**Theorem 23.2** (Schöning 1999). There is an absolute constant \( c > 0 \) such that

\[
p(n) \geq \frac{c}{n}\left(\frac{3}{4}\right)^n.
\]

**Proof.** Let \( F \) be a satisfiable 3-CNF in \( n \) variables, and fix some (unknown for us) assignment \( a^* \) satisfying \( F \). Let \( \text{dist}(a, a^*) = |\{i : a_i \neq a_i^*\}| \) be the Hamming distance between \( a \) and \( a^* \). Since we choose our initial assignment \( a \) at random,

\[
\Pr[\text{dist}(a, a^*) = j] = \binom{n}{j}2^{-n} \quad \text{for each } j = 0, 1, \ldots, n.
\]

Hence, if \( q_j \) is the probability that the algorithm finds \( a^* \) when started with an assignment \( a \) of Hamming distance \( j \) from \( a^* \), then the probability \( q \) that the algorithm finds \( a^* \) is

\[
q = \sum_{j=0}^{n} \binom{n}{j}2^{-n}q_j.
\]

To lower bound this sum, we concentrate on the value \( j = n/3 \). As in the case of 2-CNFs, the progress of the above algorithm can be represented by a particle moving between the integers 0, 1, \ldots, \( n \) on the real line. The position of the particle indicates how many variables in the current solution have “incorrect values,” i.e., values different from those in \( a^* \). If \( C \) is a clause not satisfied by a current assignment, then \( C(a^*) = 1 \) implies that in Step (3) a “right” variable of \( C \) (that is, one on which \( a \) differs from \( a^* \)) will be picked with probability at least \( 1/3 \). That is, the particle will move from position \( i \) to position \( i - 1 \) with probability at least \( 1/3 \), and will move to position \( i + 1 \) with probability at most \( 2/3 \). We have to estimate the probability \( q_{n/3} \) that the particle reaches position 0, if started in position \( n/3 \).

Let \( A \) be the event that, during \( n \) steps, the particle moves \( n/3 \) times to the right and \( 2n/3 \) times to the left. Then

\[
q_{n/3} \geq \Pr[A] = \binom{n}{n/3}\left(\frac{1}{3}\right)^{2n/3}\left(\frac{2}{3}\right)^{n/3}.
\]

Now we use the estimate

\[
\binom{n}{\alpha n} \geq \frac{1}{O(\sqrt{n})}2^{\alpha nH(\alpha)} \geq \frac{1}{\Theta(\sqrt{n})}\left[\left(\frac{1}{\alpha}\right)^\alpha\left(\frac{1}{1-\alpha}\right)^{1-\alpha}\right]^n,
\]

where \( 0 < \alpha < 1 \) is the fraction of clauses in \( F \) that are satisfiable. To prove this, we use

\[
\binom{n}{\alpha n} \geq \frac{1}{(1-\alpha)^{\alpha n}}\left[\frac{1}{\alpha}\right]^{\alpha n} = \frac{1}{\Theta(\sqrt{n})}\left[\frac{1}{\alpha}\right]^{\alpha n}\left[\frac{1}{1-\alpha}\right]^{1-\alpha n},
\]

and

\[
\frac{1}{\alpha^{\alpha n}}\left[\frac{1}{1-\alpha}\right]^{1-\alpha n} \geq \frac{1}{\Theta(\sqrt{n})}\left[\left(\frac{1}{\alpha}\right)^\alpha\left(\frac{1}{1-\alpha}\right)^{1-\alpha}\right]^n.
\]
where $H(\alpha) = -\alpha \log_2 \alpha - (1 - \alpha) \log_2 (1 - \alpha)$ is the binary entropy function (see Exercise 1.16). Therefore, setting $\alpha = 1/3,$

$$q \geq \binom{n}{n/3} g_{n/3} 2^{-n} \geq \binom{n}{n/3}^2 \left( \frac{1}{3} \right)^{2n/3} \left( \frac{2}{3} \right)^{n/3} 2^{-n} \geq \frac{1}{\Theta(n)} \left[ 3^{2/3} \left( \frac{3}{2} \right)^{4/3} \left( \frac{1}{3} \right)^{2/3} \left( \frac{2}{3} \right)^{1/3} 2^{-1} \right]^n = \frac{1}{\Theta(n)} \left( \frac{3}{4} \right)^n. \quad \square$$

### 23.2 Random walks in linear spaces

Let $V$ be a linear space over $\mathbb{F}_2$ of dimension $d$, and let $v$ be a random vector in $V$. Starting with $v$, let us “walk” over $V$ by adding independent copies of $v$. (Being an independent copy of $v$ does not mean being identical to $v$, but rather having the same distribution.) What is the probability that we will reach a particular vector $v \in V$? More formally, define

$$v^{(r)} = v_1 \oplus v_2 \oplus \cdots \oplus v_r,$$

where $v_1, v_2, \ldots, v_r$ are independent copies of $v$. What can be said about the distribution of $v^{(r)}$ as $r \to \infty$? It turns out that, if $\Pr[v = 0] > 0$ and $v$ is not concentrated in some proper subspace of $V$, then the distribution of $v^{(r)}$ converges to a uniform distribution, as $r \to \infty$. That is, we will reach each vector of $V$ with almost the same probability!

**Lemma 23.3** (Razborov 1988). Let $V$ be a $d$-dimensional linear space over $\mathbb{F}_2$. Let $b_1, \ldots, b_d$ be a basis of $V$ and

$$p = \min \{ \Pr[v = 0], \Pr[v = b_1], \ldots, \Pr[v = b_d] \}.$$

Then, for every vector $u \in V$ and for all $r \geq 1$,

$$\left| \Pr[v^{(r)} = u] - 2^{-d} \right| \leq e^{-2pr}.$$

**Proof.** Let $(x, y) = x_1 y_1 \oplus \cdots \oplus x_n y_n$ be the scalar product of vectors $x, y$ over $\mathbb{F}_2$; hence $(x, y) = 1$ if and only if the vectors $x$ and $y$ have an odd number of 1s in common. For a vector $w \in V$, let $p_w = \Pr[v = w]$ and set

$$\Delta_v := \sum_{w \in V} p_w (-1)^{(w, v)}. \quad (23.1)$$