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

$$\begin{aligned} x(0) &= 0, \\ x(i) &= \frac{x(i-1)+x(i+1)}{2} + 1, \\ x(n) &= x(n-1) + 1. \end{aligned}$$

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. □

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 assignment 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 random? If a formula is satisfiable, then we will "catch" a satisfying assignment with probability at least 2^{-n}. Interestingly, the success probability can be substantially increased to about $(3/4)^n$ via the following simple algorithm proposed by Schöning (1999):

1. Pick an initial assignment $a \in \{0,1\}^n$ uniformly at random. The assignment a can be obtained as a result of n independent experiments, where at the i-th experiment we flip a coin to determine the i-th bit of a.
2. If a satisfies all clauses of F, then stop with the answer "F is satisfiable."
3. If F is not satisfied by a, then pick any of its unsatisfied clauses C, choose one of C's literals uniformly at random, flip its value, and go to step (2).
4. Repeat (3) n times.

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 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 $(1-p)^t \leq \mathrm{e}^{-pt} = \mathrm{e}^{-30}$, 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 $\mathrm{dist}(a, a^*) = |\{i : a_i \neq a_i^*\}|$ be the Hamming distance between a and a^*. Since we choose our initial assignment a at random,

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

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

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

where $H(\alpha) = -\alpha \log_2 \alpha - (1-\alpha)\log_2(1-\alpha)$ is the binary entropy function (see Exercise 1.16). Therefore, setting $\alpha = 1/3$,

$$\begin{aligned} q &\geq \binom{n}{n/3} q_{n/3} 2^{-n} \\ &\geq \binom{n}{n/3}^2 \left(\frac{1}{3}\right)^{2n/3} \left(\frac{2}{3}\right)^{n/3} 2^{-n} \\ &\geq \frac{1}{\Theta(n)} \left[3^{2/3} \left(\frac{3}{2}\right)^{4/3} \left(\frac{1}{3}\right)^{2/3} \left(\frac{2}{3}\right)^{1/3} 2^{-1} \right]^n \\ &= \frac{1}{\Theta(n)} \left(\frac{3}{4}\right)^n . \end{aligned}$$ □

23.2 Random walks in linear spaces

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

$$\boldsymbol{v}^{(r)} = \boldsymbol{v}_1 \oplus \boldsymbol{v}_2 \oplus \cdots \oplus \boldsymbol{v}_r ,$$

where $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_r$ are independent copies of $\boldsymbol{v}$. What can be said about the distribution of $\boldsymbol{v}^{(r)}$ as $r \to \infty$? It turns out that, if $\Pr[\boldsymbol{v} = 0] > 0$ and $\boldsymbol{v}$ is not concentrated in some proper subspace of V, then the distribution of $\boldsymbol{v}^{(r)}$ 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*

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

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

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

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

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