decomposed into $m-1$ chains. These chains, together with $\{a, b\}$, give a decomposition of P into m chains. □

3.2.1 The marriage problem

Dilworth's theorem will be considered further in Chapter 13. Meanwhile we close this section by showing how it can be used to give an alternative proof of the marriage theorem (Theorem 2.2.1).

Proof Let $A_1, \ldots, A_m$ be $m \leqslant n$ subsets of $S = \{x_1, \ldots, x_n\}$ such that, for each $k \leqslant m$, any k sets A_i contain at least k elements in their union. Define a poset as follows: take objects $u_1, \ldots, u_n$ and $v_1, \ldots, v_m$ and define an order relation by

$$\begin{aligned} u_i &\leqslant v_j \quad \text{if and only if } x_i \in A_j \\ u_i &\nleqslant u_j \quad \text{if } i \neq j \\ v_i &\nleqslant v_j \quad \text{if } i \neq j. \end{aligned}$$

It can be seen that u_i is really representing x_i and v_i is representing A_i. Now $\{u_1, \ldots, u_n\}$ is an antichain in P, and we now show that it is a maximum-sized antichain. Suppose, after a suitable relabelling if necessary, that $\{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ is an antichain. Then none of $x_1, \ldots, x_r$ is in any of $A_1, \ldots, A_s$, so the only possible elements of $A_1, \ldots, A_s$ are $x_{r+1}, \ldots, x_n$. Thus the s sets $A_1, \ldots, A_s$ have $\leqslant n-r$ elements in their union. However, they have $\geqslant s$ elements in their union, so we must have $s \leqslant n-r$, i.e. $r+s \leqslant n$. Therefore n is indeed the maximum size of an antichain. It now follows from Dilworth's theorem that P can be decomposed into n chains. Each chain must contain exactly one u_i. Since the v_j are all in different chains, there corresponds to each v_j a u_j in the same chain with $u_j \leqslant v_j$; thus to each A_j there corresponds an x_j with $x_j \in A_j$. □

3.3 Symmetric chains for sets

Having looked at symmetric chains in a more general setting, we are now going to return to the particular case of subsets of a set and examine the structure of the chains more closely. Suppose we wish to find a symmetric chain decomposition of the set of subsets of a given set. The construction given in the proof of Theorem 3.1.1 is a step-by-step construction, altering the chains at each step. This makes for a tedious construction if the given set is large. Is there a neater way of writing down the chains without having to find the chains for all the smaller sets in the process? A positive answer to this question has been given by Leeb (pers. comm.) and, independently, by Greene and Kleitman (1976*b*).

Corresponding to each subset A of $S = \{x_1, \ldots, x_n\}$ we associate a sequence of n parentheses. If $x_i \in A$ we put a right parenthesis in the ith place; if $x_i \notin A$ we put a left parenthesis in the ith place. For example, if $S = \{1, \ldots, 9\}$ and $A = \{2, 3, 4, 7, 8\}$ we represent A by

$$(\,)\,)\,)\,(\,(\,)\,)\,(\,.$$

Having done this we can now 'close' the brackets as far as possible. In the example given, we obtain

$$\underbrace{(\,)}\,)\,)\,\underbrace{(\,\underbrace{(\,)}\,)}\,(\,.$$

Elements of S which correspond to right parentheses which are paired in the closing process are called the *basic elements* of A. In the example 2, 7 and 8 are the basic elements of A. The unpaired right parentheses represent non-basic elements of A. Note that all unpaired left parentheses must occur to the right of all the unpaired right parentheses, for otherwise further closing of brackets would be possible. These unpaired left parentheses represent unpaired elements of the complement A'.

Now define A^- to be the set of basic elements of A, and A^+ to be the union of A with the set of unpaired elements of A'. Then

$$\begin{aligned} |A^+| &= |A| + |A'| - \text{number of paired elements of } A' \\ &= |S| - \text{number of paired elements of } A \\ &= |S| - |A^-| \end{aligned}$$

so that $|A^-| + |A^+| = |S|$.

Now form a chain containing A by starting with A^-, the set of basic elements of A, and adding one by one the non-basic elements of A in order, and then adding one by one the unpaired elements of A' in order. The chain therefore starts with A^-, contains A, and ends with A^+. Since $|A^-| + |A^+| = |S|$, the chain is a *symmetric* chain containing A. In the example above, the basic elements of A are 2, 7, 8, and the elements 3, 4, 9 are added in turn to give the chain

$$\{2,7,8\} \subset \{2,3,7,8\} \subset \{2,3,4,7,8\} \subset \{2,3,4,7,8,9\}. \quad (3.2)$$

The reader could check that this is one of the chains which the proof of Theorem 3.1.1 would construct!

In terms of parentheses, the basic elements determine all the closed parentheses uniquely and leave all the unpaired parentheses to be fitted in. The chains are constructed by first taking all the unpaired parentheses as left ones (giving A^-), then changing the first of them to a right parenthesis, then the second, and so on. The chain (3.2) is, in terms of parentheses,

$$
\begin{array}{l}
\underbracket{(\,)}\ (\ (\ \underbracket{(\ \underbracket{(\,)}\ )}\ (\\
\underbracket{(\,)}\ )\ (\ \underbracket{(\ \underbracket{(\,)}\ )}\ (\\
\underbracket{(\,)}\ )\ )\ \underbracket{(\ \underbracket{(\,)}\ )}\ (\\
\underbracket{(\,)}\ )\ )\ \underbracket{(\ \underbracket{(\,)}\ )}\ )\ .
\end{array}
$$

Observe how the closed parts remain unchanged while the remaining parts change step by step from left to right parentheses.

If two subsets of S have the same basic elements, they will have the same closed parts and hence will give rise to (and be contained in) the same chain. The set of all chains obtained in this way forms a symmetric chain decomposition of the set of subsets of S; every set lies in a chain, and the chains are disjoint since they are each determined by basic elements and each subset has a unique set of basic elements.

We can now see that the chains formed in this way are precisely those obtained in Theorem 3.1.1. For small values of n we could find the chains explicitly and verify this; therefore we proceed with an induction argument. Suppose that the chains of Theorem 3.1.1 for an n-set are the same as those of the parenthesis construction, and consider how the chains for an $(n+1)$-set are formed. The first new chain in the de Bruijn construction is obtained by extending an existing chain by adjoining x_{n+1} to its final set:

$$
\begin{array}{cccc|c}
A_1 & A_2 & \dots & & A_h \\
\hline
A_1 \cup \{x_{n+1}\} & A_2 \cup \{x_{n+1}\} & \dots & & A_h \cup \{x_{n+1}\}
\end{array}
$$

This corresponds to appending '(' to each string of parentheses representing the sets $A_1, \dots, A_h$ and then changing it to ')' to represent $A_h \cup \{x_{n+1}\}$. The resulting chain is precisely a chain of subsets of $\{x_1, \dots, x_{n+1}\}$ with the same basic elements as those of the original chain. The second new chain formed from $A_1 \subset \dots \subset A_h$ is obtained by appending x_{n+1} to each of $A_1, \dots, A_{h-1}$, i.e. appending ')' to the strings of parentheses representing $A_1, \dots, A_{h-1}$. The fact that A_h is omitted corresponds to making the last non-basic element, say x_j, of A_h no longer available. This is achieved by forming a closed pair of brackets, '(' at the jth place and ')' at the $(n+1)$th place; therefore the resulting chain consists of all subsets of $\{x_1, \dots, x_{n+1}\}$ whose basic elements are precisely those of the original chain together with x_{n+1}. Thus again the new chain consists of subsets with the same basic elements.

The chains possess some elementary properties which are worth recording.

Theorem 3.3.1 Let $A_1 \subset \dots \subset A_r$ be one of the symmetric chains of subsets of the n-set S constructed as above.

(i) If $A_{i+1} = A_i \cup \{x_{m_i}\}$, then $m_i < m_{i+1}$ for each i, and the m_i are alternatively odd and even.

(ii) The number of basic elements in each of the A_i is $\frac{1}{2}(n+1-r)$.

(iii) For each i, there is a set B_i such that $A_{i-1} \subset B_i \subset A_{i+1}$ and with B_i in a *shorter* chain.

Proof (i) That $m_i < m_{i+1}$ is immediate from the construction. Note also that any block of closed parentheses must contain an even number of elements, so that $m_{i+1} = m_i + (\text{even number}) + 1$.

(ii) We have

$$
\begin{aligned}
n &= (\text{number of paired elements}) \\
&\quad + (\text{number of unpaired elements}) \\
&= 2(\text{number of basic elements}) \\
&\quad + (\text{number of unpaired elements}).
\end{aligned}
$$

Now the chain is constructed by adding one unpaired element at a time, so that the number of unpaired elements must be $r-1$. Therefore

$$n = 2(\text{number of basic elements}) + r - 1.$$

(iii) The sequences of parentheses representing A_{i-1} and A_{i+1} differ in two places. We have

$$
\begin{aligned}
A_{i-1}&: \dots\ (\ \mathrm{XX}\ (\ \dots \\
A_i&: \dots\ )\ \mathrm{XX}\ (\ \dots \\
A_{i+1}&: \dots\ )\ \mathrm{XX}\ )\ \dots
\end{aligned}
$$

where XX denotes a (possibly empty) closed part. Consider the subset B_i represented by

$$B_i: \dots\ (\ \mathrm{XX}\ )\ \dots .$$

It clearly satisfies $A_{i-1} \subset B_i \subset A_{i+1}$. Also, since a further bracketing is now possible in the sequence for B_i it follows that B_i has more basic elements than A_i, and so, by part (ii), the chain in which it lies is shorter. □

There are yet more equivalent ways of constructing the same symmetric chain decompositions as those described above, and we briefly mention two of these. If we look at, for example, the 2-subsets of $\{1, \ldots, 4\}$ in lexicographic order (alphabetical, with 1 in place of a, 2 in place of b, etc.), and assign to each the first available 3-set containing it we obtain

$\{1,2\}$–$\{1,2,3\}$
$\{1,3\}$–$\{1,3,4\}$
$\{1,4\}$–$\{1,2,4\}$
$\{2,3\}$–$\{2,3,4\}$
$\{2,4\}$–none left
$\{3,4\}$–

Note that this is precisely the pairing between 2-subsets and 3-subsets in the symmetric chain decomposition of Example 3.1. Aigner (1973) has shown that this always holds, so that the chains can be built up rank by rank.

Another approach is due to White and Williamson (1977). To find out which set covers the set $\{a_1, \ldots, a_h\}$ in its chain, work out $a_i - 2i$ for each i (taking $a_0 = 0$) and define t to be the largest interger i, $0 \leq i \leq h$, for which $a_i - 2i$ is minimal; then the set covering $\{a_1, \ldots, a_h\}$ in its chain is $\{a_1, \ldots, a_h, 1 + a_t\}$. For example, to find the set covering $\{2, 3, 7, 8\}$, work out $0 - 2.0 = 0$, $2 - 2.1 = 0$, $3 - 2.2 = -1$, $7 - 2.3 = 1$, and $8 - 2.4 = 0$; take $t = 2$ to obtain the set $\{2, 3, 4, 7, 8\}$ since $1 + a_2 = 1 + 3 = 4$.

3.4 Applications

We now give some applications of the symmetric chain structure.

3.4.1 The number of antichains

Given an n-set S, how many antichains of subsets of S are there? We shall accept as antichains two rather dubious candidates, namely the empty antichain which contains no subsets and the antichain consisting of only the empty set. This is to enable us to formulate an equivalent version of the question posed above.

We show that antichains of subsets of S are in one–one correspondence with increasing functions from $\mathscr{P}(S)$, the set of subsets of S, to $\{0, 1\}$. Here we say that a function $f: \mathscr{P}(S) \to \{0, 1\}$ is *increasing* if $f(X) \leq f(Y)$ whenever $X \subseteq Y$. Given an antichain $\mathscr{A}$, we can define $f: \mathscr{P}(S) \to \{0, 1\}$ by $f(B) = 0$ if B is a subset of a member of $\mathscr{A}$ and $f(B) = 1$ otherwise. To check that this f is increasing we need only check that if $B \subset D$ and $f(D) = 0$ then $f(B) = 0$. However, if $f(D) = 0$ then $D \subseteq A$ for some $A \in \mathscr{A}$; then $B \subseteq A$ also, so $f(B) = 0$.

It is clear that under this correspondence the sets in the antichain are precisely the maximal sets on which f takes the value zero. Conversely, given an increasing function $f: \mathscr{P}(S) \to \{0, 1\}$, the maximal sets on which f takes the value zero will form an antichain. Thus the required correspondence has been exhibited. Note that the empty antichain corresponds to the function f which takes the value unity everywhere.

The number of antichains is therefore the number of ways of defining an increasing function $f: \mathscr{P}(S) \to \{0, 1\}$. We therefore consider the problem of constructing as many increasing functions as we can. Suppose that we decompose the set of subsets of S into symmetric chains, and that we attempt to construct f by defining it on the sets in one chain at a time. More precisely, suppose that we have succeeded in defining an increasing function f consistently on all chains of size less than k and that we now attempt to extend the definition of f to a given chain of size k.

If $k = 2$, any chain of size k is of the form $X \subset Y$. Here there are at most three possible choices of values for $f(X)$ and $f(Y)$: we could have $f(X) = f(Y) = 0$, or $f(X) = f(Y) = 1$, or $f(X) = 0$ and $f(Y) = 1$. Certainly the choice $f(X) = 1$, $f(Y) = 0$ is not allowed. Thus there are at most three possibilities.

If $k > 2$, consider any two sets X, Y in the chain under consideration with $|Y| = |X| + 2$. We then have

$$\ldots X \subset Z \subset Y \ldots$$

for some set Z. Now by Theorem 3.3.1(iii) there is a set U, $X \subset U \subset Y$, with U in a shorter chain, and hence with $f(U)$ already defined. It follows that if the chain

$$X_1 \subset X_2 \subset \ldots \subset X_k$$

is being considered, then, for each $i = 2, \ldots, k-1$, there is a set U_i such that $X_{i-1} \subset U_i \subset X_{i+1}$ and with $f(U_i)$ already defined. If $f(U_i) = 0$ for all i, $2 \leq i \leq k-1$, then we must take $f(X_{i-1}) = 0$ for each $i \leq k-1$ and we are possibly free to define f on X_{k-1} and X_k. As before, there are at most three possible choices here, $f(X_{k-1}) = 1$, $f(X_k) = 0$ not being allowed. So again there are at most three possible ways of final part of some $\bar{V}_f$: thus A occurs in the above sequence as part of $\bar{V}_f U_e$. Thus the sequence contains every subset of S as required. The length of the sequence is

$$\leqslant 2m^2(k+1) = 2(k+1)\binom{k}{[k/2]}^2.$$

However,

$$\binom{k}{[k/2]} \approx \left(\frac{2}{k\pi}\right)^{1/2} 2^k$$

by Stirling's approximation, so that

$$2m^2(k+1) \approx \frac{4}{k\pi} \cdot 2^{2k} \cdot k = \frac{4}{\pi} 2^n.$$

This estimate for the length of the sequence can be halved by using Exercise 3.10, thus proving the theorem.
The proof for n odd is similar. □

3.4.3 A probability result related to Sperner's theorem

Another application of the symmetric chain structure leads to an elegant probabilistic version of Sperner's theorem. We investigate the following problem. Suppose that two subsets A, B are chosen independently and at random from the set of subsets of an n-set S, and suppose that the underlying probabilities of each being chosen are known. Then what can be said about the probability that $A \subseteq B$? We shall show that, no matter what the underlying probability distribution is, the probability that $A \subseteq B$ is at least $1\Big/\binom{n}{[n/2]}$.

Lemma 3.4.3 Let $p_1, \ldots, p_m$ be a probability distribution on an m-element set T. Then the probability that two elements of T chosen at random are identical is $\geqslant 1/m$, irrespective of the p_i.

Proof The required probability is $\sum_{i=1}^m p_i^2$. Now we clearly have

$$\sum_{i=1}^m \left(p_i - \frac{1}{m}\right)^2 \geqslant 0$$

so

$$\sum_{i=1}^m p_i^2 - \frac{2}{m}\sum_{i=1}^m p_i + m \cdot \frac{1}{m^2} \geqslant 0$$

whence

$$\sum_{i=1}^m p_i^2 \geqslant \frac{2}{m}\sum_{i=1}^m p_i - \frac{1}{m} = \frac{2}{m} - \frac{1}{m} = \frac{1}{m}.$$ □

Lemma 3.4.4 If $\{q(x)\}$ is a probability distribution on a poset P and P is partitioned into m chains, then the probability that two elements of P chosen at random lie in the same chain is $\geqslant 1/m$, no matter what the values of q are.

Proof In Lemma 3.4.3 take T to be the set of chains. The required probability is the probability of choosing two chains at random and obtaining the same chain twice. The probability p_i of choosing the ith chain is given by $p_i = \sum q(x)$ where the summation is over all x in the ith chain. The result is immediate from Lemma 3.4.3. □

Note that the probability that two elements chosen at random lie in the same chain can be written as

$$\sum_{x\in P} q(x)\Bigg(\sum_{\substack{y\\ x,\,y \text{ in}\\ \text{same chain}}} q(y)\Bigg) = \sum_x q^2(x) + 2\sum_{\substack{x<y\\ x,\,y \text{ in}\\ \text{same chain}}} q(x)q(y).$$

Therefore the result of Lemma 3.4.4 can be written as

$$\sum_x q^2(x) + 2\sum_{\substack{x<y\\ x,\,y \text{ in}\\ \text{same chain}}} q(x)q(y) \geqslant \frac{1}{m}.$$

Suppose now that we can find two chain decompositions of P into m chains with the property that no pair of elements of P in the same chain in one of the decompositions lies in the same chain in the second decomposition. (Such a pair of chain decompositions are said to be *orthogonal*.) We can then obtain an inequality as above for both the chain decompositions, and on adding them together and dividing by 2 we obtain

$$\sum_x q^2(x) + \sum{}^* q(x)q(y) \geqslant \frac{1}{m}$$

where $\sum^*$ denotes the sum over all x, y such that $x<y$ and x, y occur in the same chain in one of the two decompositions. Since

$$\sum{}^* q(x)q(y) \leqslant \sum_{x<y} q(x)q(y)$$

we therefore have

$$\sum_x q^2(x) + \sum_{x<y} q(x)q(y) \geqslant \frac{1}{m}. \tag{3.3}$$

We can now prove the following theorem.

Theorem 3.4.5 (Baumert, McEliece, Rodemich, and Rumsey 1980) If two sets A, B are chosen independently according to a probability distribution defined on the subsets of an n-set S, then the probability that $A \subseteq B$ is at least $1\Big/\binom{n}{[n/2]}$.

Proof Take $m = \binom{n}{[n/2]}$. The required probability is

$$\sum_A q^2(A) + \sum_{A \subset B} q(A)q(B)$$

where $q(A)$ is the probability of choosing A. Thus, by (3.3), the probability is $\geqslant 1/m$—provided of course that an orthogonal pair of chain decompositions exists! This is now proved. □

Theorem 3.4.6 (Shearer and Kleitman 1979) If $n \geqslant 2$, there exist two orthogonal chain decompositions of the poset of subsets of an n-set into $\binom{n}{[n/2]}$ chains.

Proof If $n = 2$ or 3 it is easy to find such decompositions (see Exercise 3.11). Therefore we now suppose that $n \geqslant 4$.

First of all take the symmetric chain decomposition constructed earlier in this chapter. Then obtain another chain decomposition by replacing each set by its complement. Certainly $\varnothing$ and S will lie in the same chain in both decompositions, but we show that no other pair of sets have that property. If A, B with $A \subset B$ lie in the same chain in both decompositions then A and B must have the same basic elements and their complements A' and B' must also have the same basic elements. Also, the string of parentheses representing A' is obtained from the string representing A by replacing all left parentheses by right ones and vice versa. We now study the strings for A and B and show that if A and B have the same basic elements, then A' and B' cannot have the same basic elements except when A and B are $\varnothing$ and S.

Suppose first that A is not the smallest set in its chain. Then with A and B in the same chain and $A \subset B$, we must have the following strings of parentheses:

$$A\colon\ C_0\ )\ C_1 \ldots\ )\ C_i\ (\ C_{i+1} \ldots$$
$$B\colon\ C_0\ )\ C_1 \ldots\ )\ C_i\ )\ C_{i+1} \ldots$$

where the C_i respresent (possibly empty) closed parts. Since A is not the smallest set in its chain, there is at least one ')' before C_i. Now the strings representing A' and B' are obtained by interchanging left and right parentheses, and it is clear that this interchange applied to the string for A will result in the reversed bracket between C_i and C_{i+1} closing with a previous bracket whereas this closing will not take place in the case of B. Thus A' and B' do not have the same closed parts.

A similar argument applies if B is not the last set in its chain. We are left with the case when A and B are the first and last members of their chain. We then have

$$A\colon\ C_0\ (\ C_1\ (\ \ldots$$
$$B\colon\ C_0\ )\ C_1\ )\ \ldots$$

If there is a non-empty C_i to the left of a '(' in A then on reversal there will be a closing of brackets in A which will not occur in B. If there is a non-empty C_i to the right of a ')' in B then there will, on reversal, be a closing of brackets in B which will not occur in A. Thus, unless all C_i are empty (in which ase $A = \varnothing$ and $B = S$), A' and B' will have different closed parts and hence different basic elements.

The two symmetric chain decompositions are therefore almost orthogonal. To make them orthogonal, we remove $\varnothing$ from its chain in the first decomposition and add it to any chain which does not contain any of the $n-1$ sets other than S or itself in its chain in the other decomposition. This is possible since there are more than n chains if $n > 3$. □

3.5 Nested chains

In obtaining a generalization of Sperner's theorem, Lih (1980) considered collections $\mathscr{A}$ of subsets of an n-set S which are not only antichains but which have the further property that every member of $\mathscr{A}$ has a non-empty intersection with a given k-element subset T of S. The case $k = n$, i.e. $T = S$, clearly reduces to Sperner. Lih showed that $\mathscr{A}$ has the Sperner property, so that

$$|\mathscr{A}| \leqslant \max_i \{\text{no. of subsets of size } i \text{ which intersect } T\}$$
$$= \max_i \left\{\binom{n}{i} - \binom{n-k}{i}\right\}$$

since the number of i-subsets of S which do *not* intersect T is $\binom{n-k}{i}$.

It is not hard to check that the maximum occurs when $i = [\tfrac{1}{2}n]$ (see