第30卷第3期 数 学 进 展 Vol.30, No.3
2001年6月 ADVANCES IN MATHEMATICS June, 2001

可满足性 (SAT) 问题的概率研究

张奎 陈大岳

(北京大学数学科学学院概率统计系, 北京, 100871, 中国)

021 A

摘要 本文首先构造了随机均匀产生的 d-SAT 问题的概率模型; 然后给出了 SAT 问题的解的个数的均值的计算公式. 使用矩方法研究了解空间的元素满足方程的概率以及在临界点方程有解的概率的极限性质. 最后确定了 $n/m = r_d = (\ln 2)/(\ln \frac{2^d}{2^d-1})$ 是其解的平均个数的临界点, 并且当 $n/m = r_d$ 时, 方程有解的概率随着 $m \to \infty$ 而趋于 0.

关键词 SAT 问题; 相变现象; 可满足概率

MR(1991) **主题分类** 60C05, 03B05

1 引言

可满足性 (satisfiability, 简记为 SAT) 问题是解决数理逻辑、推理、机器学习等许多理论问题与实际问题的基础性问题. SAT 问题是第一个被发现的 NP 完全问题 [9], 也是一大类 NP 完全问题的核心. 因此, 求解 SAT 问题在研究人工智能系统和计算理论中有着很重要的作用. 而对于随机均匀产生的 SAT 问题研究其概率性质, 可以确定问题的难易分布 [7,15], 不仅有其在理论上的重要意义, 对于设计有效的算法也有重要意义.

SAT 问题由三个要素组成 [2,9,11]:

- m 个逻辑变量 (variable) 的集合: $x_1, x_2, \cdots, x_m$;
- 基本式 (literal) 的集合: 一个基本式就是一个逻辑变量或其非. 这样, 全部基本式为: $x_1, \overline{x}_1, x_2, \overline{x}_2, \cdots, x_m, \overline{x}_m$;
- n 个子句 (clause) 的集合: $C_1, C_2, \cdots, C_n$; 其中每个子句是由逻辑或 ($\vee$) 连接的基本式组成, 子句中基本式的个数称为子句的长度. 例如, $C = x_1 \vee \overline{x}_3 \vee x_7$ 就是一个长度为 3 的子句.

所谓 SAT 问题就是确定是否存在一组变量的逻辑取值使得合取范式 $C_1 \wedge C_2 \wedge \cdots \wedge C_n$ 的值为真. 若每个子句 C_i 的长度均为 d, 则称为 d-SAT 问题. 在研究或求解 d-SAT 问题时, 通常需要预先指定实例模型. 本文所研究的是随机均匀产生的 d-SAT 实例模型, 即每个子句均匀独立地随机产生; 每个子句由 d 个基本式组成, 且这 d 个基本式所代表的逻辑变量不同; 每个基本式在各个子句中出现的概率相同. 这个模型被很多研究者所采用 [7,12,13,15,16].

在本文中, 我们首先构造了概率空间, 对上述随机均匀产生的 d-SAT 问题进行了概率描述; 其次, 将问题转化为一个等价形式, 对可满足概率、解的平均个数进行了研究; 最后, 求出了在临界点的可满足概率.

2 基本概念与主要结果

假设 d 维随机向量 $L_1, L_2, \cdots, L_n$ 独立同分布, L 的每个分量取值于 $\{1, 2, \cdots, m\}$, 其概

收稿日期: 1998-10-28. 收到修改稿日期: 1999-5-24.
国家教委博士点基金, 资助优秀青年教师基金, 自然科学基金重点项目和国家八六三高科技项目资助.

率分布为

$$P(L=(i_1,i_2,\cdots,i_d))=\begin{cases}\dfrac{1}{d!C_m^d}, & i_1,\cdots,i_d\text{互不相同;}\\ 0, & i_1,\cdots,i_d\text{有相同者.}\end{cases}$$

又设随机变量族 $\{\alpha_{kj};1\le k\le n;1\le j\le d\}$ 独立同分布，且与随机向量族 $L_1,L_2,\cdots,L_n$ 相互独立，其概率分布为

$$P(\alpha_{kj}=1)=P(\alpha_{kj}=0)=1/2,\ 1\le j\le d,\quad 1\le k\le n.$$

在概率空间 $(\Omega,\mathcal{F},P)$ 中，可以进一步明确地让每一个 $\omega\in\Omega$ 对应于一组 $\{L_k,\alpha_{kj};1\le j\le d,1\le k\le n\}$. Ω 共有 $d!C_m^d2^{dn}$ 个元素，每个元素有相同的概率，即 P 是 Ω 上的均匀分布. 严格地说我们应该把 L_k, α_{kj} 写为 $L_k(\omega)$, $\alpha_{kj}(\omega)$, 但为简洁而略去 ω.

任给 $X=(x_1,x_2,\cdots,x_m)\in\{0,1\}^m$ 和 $\omega=\{L_k,\alpha_{kj};1\le j\le d,1\le k\le n\}$, 可以构造一个由 m 个逻辑变量、 n 个子句组成的 d-SAT 问题样本:

$$F_X(\omega)=(y_{L_{11}}\vee\cdots\vee y_{L_{1d}})\wedge\cdots\wedge(y_{L_{n1}}\vee\cdots\vee y_{L_{nd}}),$$

其中

$$y_{L_{kj}}=\begin{cases}x_{L_{kj}}, & \text{当}\alpha_{kj}=1\text{时;}\\ \overline{x}_{L_{kj}}, & \text{当}\alpha_{kj}=0\text{时;}\end{cases}\qquad k=1,2,\cdots,n;\quad j=1,2,\cdots,d.$$

我们可以这样理解上述 SAT 问题样本的构造. 先从 m 个逻辑变量中无放回地选取其中 d 个; 然后独立的以 $1/2$ 的概率取每个变量或其非构成一个基本式; 把三个基本式以逻辑或 $(\vee)$ 运算连接构成一个子句; 然后重复构造其余 $n-1$ 个子句, 把这 n 个子句用逻辑与 $(\wedge)$ 运算连接构成 $F_X(\omega)$. 其次, 固定 $\omega\in\Omega$, $F_X(\omega)$ 可以看作从 $\{0,1\}^m$ 到 $\{0,1\}$ 的函数. 若有 $Y\in\{0,1\}^m$ 使 $F_Y(\omega)=0$, 称此 SAT 问题有解或可满足. 求解此 SAT 问题就是求满足 $F_Y(\omega)=0$ 的 Y. 而当固定 $Y\in\{0,1\}^m$ 时, F_Y 是取值于 $\{0,1\}$ 的随机变量.

本文采用的一些记号如下:

$E=\{0,1\}^m$,

$A_X=\{\omega\in\Omega:F_X(\omega)=0\}$, 其中$X\in E$,

$S_{m,n}(\omega)=\#\{X\in E:F_X(\omega)=0\}=\sum\limits_{X\in E}I_{A_X}(\omega)$,

$M_{m,n}=\mathbf{E}S_{m,n}$,

$P_{m,n}=P\{\omega\in\Omega:\exists X\in E,\text{使}F_X(\omega)=0\}=P(\cup_{X\in E}A_X)$,

$r=n/m$,

$P_r=\lim\limits_{\substack{m\to+\infty,\\ n/m=r}}P_{m,n}$ (如果极限存在).

这些记号有着明显的意义: E 表示整个解空间; A_X 表示关于解空间 E 中元素 X 的可满足的 d-SAT 问题样本的全体; $S_{m,n}(\omega)$ 表示每个均匀产生的 d-SAT 问题样本解的个数; $M_{m,n}$ 表示均匀 d-SAT 问题的解的平均个数; $P_{m,n}$ 表示均匀 d-SAT 问题有解的概率; r 的大小表示了 SAT 问题的约束强弱, 并且 r 越大 SAT 问题越不容易有解; P_r 表示在 $n/m=r$ 条件下均匀 d -SAT 问题可满足概率的极限.

以下是本文的主要结果.

定理 1 解的平均个数是 $M_{m,n}=2^m(\frac{2^d-1}{2^d})^n$. 令 $r_d=(\ln 2)/(\ln\frac{2^d}{2^d-1})$, 则

$$\lim_{\substack{m\to+\infty\\ n/m=r}} M_{m,n}=\begin{cases}0, & r>r_d;\\ 1, & r=r_d;\\ \infty, & r<r_d.\end{cases} \tag{1}$$

定理 1 说明存在一个临界点 r_d，使得当 $r>r_d$ 时，解的平均个数以指数速度下降到 0；而当 $r<r_d$ 时，解的平均个数以指数速度增长．很多学者在研究均匀 d-SAT 问题时，发现了另一种相变现象 [4,7,10,11,16]．即存在 $0<r_0<\infty$，使当 $r<r_0$ 时，$P_r=1$；而当 $r>r_0$ 时，$P_r=0$. 但这个现象及 r_0 的值都是通过计算机模拟得到的，没有理论上的严格证明；并且在不同的文献中，这个模拟值也有所不同，但都比较接近．例如，在 d=3 时模拟的结果表明 r_d 的值在 4.3 附近．定理 1 说明均匀 d-SAT 问题解的平均个数的相变现象；并且当 $r>r_d$ 时，由 Markov 不等式，

$$P_{m,n}=P(\omega:S_{m,n}(\omega)\geq 1)\leq ES_{m,n}(\omega)=M_{m,n}.$$

由此不难得到如下推论.

推论 2　当 $r>r_d$ 时，$P_r=0$.

如前所述，是否存在 $0<r_0<\infty$，使当 $r<r_0$ 时，$P_r=1$；而当 $r>r_0$ 时，$P_r=0$，尚待进一步的研究．下面的两个定理表明如果 r_0 存在，则 $1\leq r_0\leq(\ln 2)/\ln(\frac{2^d}{2^d-1})$.

定理 3　$P_{r_d}=0$.

定理 4　当 $r<1$ 时，$P_r=1$.

定理 4 是文献 [8] 中结果的直接推论．在该文中，V. Chvâtal 和 B.Reed 研究了 2-SAT 问题的相变现象，指出子句数为 n，变量数为 m 的均匀 2-SAT 问题的临界点是 1．即，当 $n/m<1$ 时，有解的概率趋于 1；而当 $n/m>1$ 时，有解的概率趋于 0. 我们只要注意到这样一个简单的事实：对于一个均匀产生的 d-SAT 问题，随机地去掉每个子句中的 $d-2$ 个变量，则所得到的恰是一个均匀产生的 2-SAT 问题；由于在 $n/m<1$ 时，2-SAT 问题有解的概率趋于 1，因此相应的 d-SAT 问题有解的概率也趋于 1.

3 定理的证明

定理 1 的证明　为了表达及计算的方便，我们将逻辑运算改为算术运算．令

$$G_X^k(\omega)=\prod_{j=1}^{d}\left(\alpha_{kj}(1-x_{L_{kj}})+(1-\alpha_{kj})x_{L_{kj}}\right),\ k=1,2,\cdots,n.$$

则 $G_X^k(\omega)$ 只取 0,1 两个值；$G_X^k(\omega)=1$ 当且仅当 $\alpha_{kj}=1-x_{L_{kj}}$, $j=1,2,\cdots,d$. 因此

$$P\left(G_X^k(\omega)=1\right)=P\left(\alpha_{kj}=1-x_{L_{kj}},j=1,2,\cdots,d\right)=\frac{1}{2^d}.$$

而且 $F_X(\omega)=0$ 等价于对 $k=1,2,\cdots,n$ 均有 $G_X^k(\omega)=0$. 固定 $X\in E$, $1\leq k\neq j\leq n$, $G_X^k(\omega)$ 与 $G_X^j(\omega)$ 是相互独立的随机变量．因此

$$P(A_X)=P\left(\omega:G_X^k(\omega)=0,k=1,2,\cdots,n\right)=\prod_{k=1}^{n}P\left(\omega:G_X^k(\omega)=0\right)=\left(\frac{2^d-1}{2^d}\right)^n.$$

由 $M_{m,n}$ 及 $S_{m,n}(\omega)$ 的定义,

$$M_{m,n}=\mathbf{E}S_{m,n}(\omega)=\mathbf{E}\sum_{X\in E}I_{A_X}(\omega)=\sum_{X\in E}P(A_X)=2^m\left(\frac{2^d-1}{2^d}\right)^n$$
$$=\exp\left(m\ln\frac{2^d}{2^d-1}\left(\frac{\ln 2}{\ln\frac{2^d}{2^d-1}}-\frac{n}{m}\right)\right)=\exp\left(m\ln\frac{2^d}{2^d-1}(r_d-r)\right).$$

由此可推导出等式 (1).

为证明定理 3，我们需要两个引理. 设 $X=(x_1,x_2,\cdots,x_m)$, $Y=(y_1,y_2,\cdots,y_m)$, 定义 $\|X-Y\|=\sum_i|x_i-y_i|$. 如果

(i) $\sum_{i=1}^m x_i<\sum_{i=1}^m y_i$; 或

(ii) $\sum_{i=1}^m x_i=\sum_{i=1}^m y_i$时，有$x_\tau<y_\tau$, 其中 $\tau=\inf\{k:x_k\neq y_k\}$,

则称 $X<Y$.

引理 5 假设 $Y_0,Y_1,Y_2,\cdots,Y_j$ 互不相同；对任意 $1\le i\le j$, 均有 $Y_0<Y_i$, $\|Y_0-Y_i\|=1$. 则

$$P\left(A_{Y_0}\cap A_{Y_1}\cap\cdots\cap A_{Y_j}\right)=\left(\sum_{t=0}^{d}\frac{\overline{C}_j^t\overline{C}_{m-j}^{d-t}}{C_m^d}\frac{2^d-(t+1)}{2^d}\right)^n\triangleq\overline{P}_j.$$

其中

$$\overline{C}_m^j=\begin{cases}C_m^j, & j\le m;\\ 0, & j>m.\end{cases}$$

证明

$$P(A_{Y_0}\cap A_{Y_1}\cap\cdots\cap A_{Y_j})=\prod_{k=1}^{n}P\left(\omega:G_{Y_s}^k(\omega)=0,\quad 0\le s\le j\right)$$
$$=\prod_{k=1}^{n}P\left(\omega:\prod_{l=1}^{d}(\alpha_{kl}(1-y_{s,L_{kl}})+(1-\alpha_{kl})y_{s,L_{kl}})=0,\quad 0\le s\le j\right)$$
$$=\prod_{k=1}^{n}\sum_{\substack{1\le i_1,i_2,\cdots,i_d\le m\\ i_1,i_2,\cdots,i_d\ \text{互不相同}}}\frac{1}{d!C_m^d}P\left(\omega:\prod_{l=1}^{d}(\alpha_{kl}(1-y_{s,i_l})+(1-\alpha_{kl})y_{s,i_l})=0,\quad 0\le s\le j\right),$$

这里用到了 $\{L_k\}$ 和 $\{\alpha_{kj}\}$ 的独立性.

考察 $Y_s=(y_{s1},\cdots,y_{sm})$ 的分量 $\{y_{si};\,0\le s\le j,\ 1\le i\le m\}$. 可以将 $\{1,2,3,\cdots,m\}$ 分为 $I_1\cup I_2$. 当 $i\in I_1$ 时，$y_{0,i}=y_{1,i}=\cdots=y_{j,i}$. 而当 $i\in I_2$ 时，$\exists 1\le s_0\le j$, 使得 $y_{s_0,i}=1$, 而 $y_{s,i}=0, s\neq s_0, 0\le s\le j$. 显然 $|I_1|=m-j$, $|I_2|=j$. 考虑上式中的任意一项，它所取到的 $Y_0,Y_1,\cdots,Y_j$ 的某 d 个分量 $\{i_1,i_2,\cdots,i_d\}$ 所构成的 $j+1$ 个 d 维向量全体记为

$$\mathcal{H}=\{(y_{s,i_1},\cdots,y_{s,i_d}),\quad s=0,1,\cdots,j\}.$$

若 $\{i_1,i_2,\cdots,i_d\}$ 均取自 I_1, 则 $\mathcal{H}$ 只有一个元素，即 $j+1$ 个向量均相同，这时

$$P\left(\omega:\prod_{l=1}^{d}(\alpha_{kl}(1-y_{s,i_l})+(1-\alpha_{kl})y_{s,i_l})=0,\quad 0\le s\le j\right)$$
$$=P\left(\omega:\prod_{l=1}^{d}(\alpha_{kl}(1-y_{0,i_l})+(1-\alpha_{kl})y_{0,i_l})=0\right)=1-\frac{1}{2^d}.$$

这样的 $\{i_1,i_2,\cdots,i_d\}$, 如果计算不同排序的话，共有 $d!\overline{C}_{m-j}^{d}$ 个.

若 $\{i_1,i_2,\cdots,i_d\}$ 中有一个取自 I_2, 其余均取自 I_1, 则 $\mathcal{H}$ 只有两个元素. 不妨设 $Y_0\neq Y_1$, 则 $(\omega:G_{Y_0}^{k}(\omega)=1)$ 与 $(\omega,G_{Y_1}^{k}(\omega)=1)$ 不能同时发生. 因此

$$\begin{aligned}&P\Big(\omega:\prod_{l=1}^{d}\big(\alpha_{kl}(1-y_{s,i_l})+(1-\alpha_{kl})y_{s,i_l}\big)=0,\quad 0\le s\le j\Big)\\&=1-P\Big(\omega:\prod_{l=1}^{d}\big(\alpha_{kl}(1-y_{0,i_l})+(1-\alpha_{kl})y_{0,i_l}\big)=1\Big)\\&\quad-P\Big(\omega:\prod_{l=1}^{d}\big(\alpha_{kl}(1-y_{1,i_l})+(1-\alpha_{kl})y_{1,i_l}\big)=1\Big)=1-\frac{2}{2^d}.\end{aligned}$$

这样的 $\{i_1,i_2,\cdots,i_d\}$, 如果计算不同排序的话，共有 $d!\overline{C}_{m-j}^{d-1}\overline{C}_{j}^{1}$ 个.

一般说来，若 $\{i_1,i_2,\cdots,i_d\}$ 中有 t 个取自 I_2, 其余 $d-t$ 取自 I_1, 则 $\mathcal{H}$ 只有 $t+1$ 个元素. 这时

$$P\Big(\omega:\prod_{l=1}^{d}\big(\alpha_{kl}(1-y_{s,i_l})+(1-\alpha_{kl})y_{s,i_l}\big)=0,\quad 0\le s\le j\Big)=1-\frac{t+1}{2^d}.$$

这样的 $\{i_1,i_2,\cdots,i_d\}$, 如果计算不同排序的话，共有 $d!\overline{C}_{m-j}^{d-t}\overline{C}_{j}^{t}$ 个.

总结前面的分析，我们得到

$$\begin{aligned}P(A_{X_i}\cap A_{X_1^j}\cap\cdots\cap A_{X_j^j})&=\prod_{k=1}^{n}\sum_{\substack{i_1,\cdots,i_d=1\\ i_1,\cdots,i_d\ \text{互不相同}}}^{m}\frac{1}{d!C_m^d}\sum_{t=0}^{d}\Big(1-\frac{t+1}{2^d}\Big)d!\overline{C}_{m-j}^{d-t}\overline{C}_{j}^{t}\\&=\Big(\sum_{t=0}^{d}\frac{\overline{C}_{j}^{t}\overline{C}_{m-j}^{d-t}}{C_m^d}\frac{2^d-(t+1)}{2^d}\Big)^n.\end{aligned}$$

引理 6

$$P_{m,n}\le 2^m\Big(\frac{2^d-1}{2^d}\Big)^n-\Big(2^m-\sum_{j=0}^{k}C_m^j\Big)\Big(\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\Big).$$

其中 k 是正整数，$1\le k\le m$，$\overline{P}_j$ 的定义如同引理 5.

证明　根据前面定义的序，对 E 中的元素从小到大排序，每一个元素对应一个序号，记为 $\{X_1,X_2,\cdots,X_{2^m}\}$. E 还可以分解成如下 $m+1$ 个集合.

$$E=E_0\cup E_1\cup\cdots\cup E_m,$$

其中 $E_l=\{X\in E:\sum_{j=1}^{m}x_j=l\}$;　$l=0,1,\cdots,m$. 对于 $X_i\in E_l$, $\{X_j\in E_{l+1}:\|X_j-X_i\|=1\}$ 共有 $m-l$ 个元素，记为 $Y_1,Y_2,\cdots,Y_{m-l}$. 当 $m-l\ge k+1$ 时，由 Jordan 公式及对称性可得：

于是

$$P(A_{X_i}\cap(\cup_{j=i+1}^{2^m}A_{X_j}))\geq P(\cup_{j=1}^{m-l}(A_{X_i}\cap A_{Y_j}))\geq P(\cup_{j=1}^{k+1}(A_{X_i}\cap A_{Y_j}))$$
$$=\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}P(A_{X_i}\cap A_{Y_1}\cap\cdots\cap A_{Y_j})=\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j.$$

最后一步利用了引理 5（以 X_i 为 Y_0）. 于是

$$\begin{aligned}P_{m,n}&=P\left(\cup_{i=1}^{2^m}A_{X_i}\right)=P(A_{X_1})+P\left(\cup_{i=2}^{2^m}A_{X_i}\right)-P\left(A_{X_1}\cap(\cup_{i=2}^{2^m}A_{X_i})\right)\\&=P(A_{X_1})+P(A_{X_2})+P\left(\cup_{i=3}^{2^m}A_{X_i}\right)-P\left(A_{X_1}\cap(\cup_{i=2}^{2^m}A_{X_i})\right)-P\left(A_{X_2}\cap(\cup_{i=3}^{2^m}A_{X_i})\right)\\&=\sum_{i=1}^{2^m}P(A_{X_i})-\sum_{i=1}^{2^m-1}P\left(A_{X_i}\cap(\cup_{j=i+1}^{2^m}A_{X_j})\right)\\&=2^m\left(\frac{2^d-1}{2^d}\right)^n-\sum_{l=0}^{m}\sum_{X_i\in E_l}P\left(A_{X_i}\cap(\cup_{j=i+1}^{2^m}A_{X_j})\right)\\&\leq 2^m\left(\frac{2^d-1}{2^d}\right)^n-\sum_{l=0}^{m-(k+1)}\sum_{X_i\in E_l}P\left(A_{X_i}\cap(\cup_{j=i+1}^{2^m}A_{X_j})\right)\\&\leq 2^m\left(\frac{2^d-1}{2^d}\right)^n-\sum_{l=0}^{m-(k+1)}C_m^l\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\\&=2^m\left(\frac{2^d-1}{2^d}\right)^n-\left(2^m-\sum_{j=0}^{k}C_m^j\right)\left(\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\right).\end{aligned}$$

定理 3 的证明 当 $\frac{n}{m}=r_d$ 时，$2^m\left(\frac{2^d-1}{2^d}\right)^n=1$，由引理 6 可知

$$\begin{aligned}P_{m,n}&\leq 2^m\left(\frac{2^d-1}{2^d}\right)^n-\left(2^m-\sum_{j=0}^{k}C_m^j\right)\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\\&=1-\frac{2^m-\sum_{j=0}^{k}C_m^j}{2^m(\frac{2^d-1}{2^d})^n}\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\\&=1-\left(1-\sum_{j=0}^{k}C_m^j/2^m\right)\sum_{j=1}^{k+1}C_{k+1}^{j}(-1)^{j+1}\overline{P}_j\left(\frac{2^d}{2^d-1}\right)^n.\end{aligned}$$

对于固定的 k，当 $m\to\infty$ 时，$\sum_{j=0}^{k}C_m^j/2^m$ 的极限为零，而且当 $j\ll m$ 时

$$\begin{aligned}\lim_{\substack{m\to\infty,\\ n/m=r_d}}\overline{P}_j\left(\frac{2^d}{2^d-1}\right)^n&=\lim_{m\to\infty}\left(\sum_{t=0}^{d}\frac{\overline{C}_j^t\overline{C}_{m-j}^{d-t}}{C_m^d}\frac{2^d-(t+1)}{2^d-1}\right)^n\\&=\lim_{m\to\infty}\left(1-\frac{1}{2^d-1}\sum_{t=0}^{d}\frac{\overline{C}_j^t\overline{C}_{m-j}^{d-t}}{C_m^d}t\right)^{mr_d}\\&=\lim_{m\to\infty}\left(1-\frac{1}{2^d-1}\frac{dj}{m}+O\left(\frac{1}{m^2}\right)\right)^{mr_d}=\exp\left(-\frac{dj}{2^d-1}r_d\right).\end{aligned}$$

$$P_{r_d} = \lim_{\substack{m\to\infty,\\ n/m=r_d}} P_{m,n} = 1 - \sum_{j=1}^{k+1} C_{k+1}^{j}(-1)^{j+1}\exp\Big(-\frac{dj}{2^d-1}r_d\Big)$$
$$= \sum_{j=0}^{k+1} C_{k+1}^{j}(-1)^{j}\exp\Big(-\frac{dj}{2^d-1}r_d\Big) = \Big(1-\exp\Big(-\frac{dr_d}{2^d-1}\Big)\Big)^{k+1}.$$

再令 $k\to\infty$, 即得 $P_{r_d}=0$.

致谢 感谢钱敏平教授的无私帮助和有益讨论. 感谢审阅者的仔细校阅.

参考文献

1 程士宏. 高等概率论. 北京: 北京大学出版社, 1994.
2 顾钧, 李国杰. 求解可满足性 (SAT) 问题的算法综述. 模式识别与人工智能, 1993, 6(2): 80-98.
3 李未, 黄文奇. 一种求解合取范式可满足性问题的数学物理方法. 中国科学, A 辑, 1994, 25(11): 1208-1217.
4 刘涛. 约束满足问题: 算法和复杂性. 中国科学院计算技术研究所博士论文, 1994.
5 Bollobâs B. Random Graphs. Academic Press, New York, 1985.
6 Chao M T and Franco J. Probabilistic analysis of a generalization of the unit-clause literal section heuristic for the K-satisfiability problem. *Information Science*, 1990, 51: 289 -324.
7 Chessman P, Karefsky B and Tayler W N. Where the really hard problems are. *Proceedings of IJCAI-1991*, 163-169.
8 Chvâtal V and Reed B. Mick gets some (the odds are his side). *Proceedings of 33rd Ann. Sypm. on Foundation of Computer Science*, 1996, 24-27.
9 Cook S A. The complexity of theorem proving procedures. *Proceedings of 3rd Ann. CM Sypm. Theory Computer*, 1971, 151-158.
10 Crawford J M and Auton L D. Experimental results on the crossover point in satisfiability problems. *The Proceedings of AAAI-1993*, 21-27.
11 Garey M R and Johnson D S. Computers and Intractability: A Guide to the Theory of Computeness. W. H. Freeman, San Francisco, 1979.
12 Jun G. Global search for satisfiability (SAT) problem. *IEEE Transactions on Knowledge and Data Engineering*, 1994, 6(3): 361-381.
13 Jun G. Local search for satisfiability (SAT) problem. *IEEE Transactions on Systems Man. and Cybernetics*, 1993, 23(4): 1108-1129.
14 Kirkaptrick S and Selman B. Critical behavior in the satisfiability of random Boolean expressions. *Science*, 1994, 264: 1297-1301.
15 Mitchell D, Selman B and Levesque H J. Hard and easy distributions of SAT problems. *Proceedings of AAAI-1992*, 459-465.
16 Selman B, Levesque H and Mitchell D. A new method for solving hard satisfiability problems. *The Proceedings of AAAI-1992*, 440-446.

A Probabilistic Study on the Satisfiability Problem

Zhang Kui Chen Dayue

(School of Math. Sciences, Peking Univ., Beijing, 100871, P. R. China)

Abstract We first define a probabilistic model for the d-satisfiability problem with each clause generated uniformly and randomly. Then we present a formula to compute the average number of solutions to a random d-satisfiability problem. We use the moment method to study the probability of an element of $\{0,1\}^m$ being a solution to a random d-satisfiability problem and the limit of the probability that a random d-satisfiability problem has a solution at the critical point. Finally we identify $n/m=r_d=(\ln 2)/(\ln\frac{2^d}{2^d-1})$ as the critical point of the average number of solutions to a random d-satisfiability problem. When $n/m=r_d$, the probability that a random d-satisfiability problem has solutions goes to 0 as $m\to\infty$.

Key words satisfiability problem; phase transition; satisfiability probability