中 国 科 学(E 辑)
第29卷 第4期 SCIENCE IN CHINA (Series E) 1999年8月

SAT 问题的相变现象*

许 可 李 未
(北京航空航天大学计算机系, 北京 100083)

摘要 相变现象是SAT问题的一个重要特性. 证明了对于随机 k-SAT模型(k为子句长度, $k \geqslant 5$), 当 r(子句数/变元数)连续增大, 到达某一个临界点时($r = r_{cr}$), 解的结构将发生与可满足概率相变类似的突变现象, 可满足赋值之间的关系突然由差别较大变得很相似.

关键词 **SAT问题 相变现象 解的结构**

合取范式的可满足性(简称SAT)问题是典型的NP完全问题[1], 其快速求解方法不仅具有重要的理论意义, 而且在软件自动化技术、逻辑推理机等领域都有直接的应用. 根据大量的实验研究, 人们猜想: 当 n 充分大以后, 对于每一个子句长度 k, 存在某个临界值 r^*, 使得当 $r < r^*$ 时, n 个变元, rn 个子句的随机 k-SAT实例可满足的概率趋近于1; 而当 $r > r^*$ 时, 其可满足的概率趋近于0, 人们称该点为跨点或"相变点", 将此现象称为SAT的相变现象[2]. 与相变现象相关的另一个性质是求解SAT实例的难度. 实验研究发现, 在相变区域两侧较远的地方, 大部分的实例都很容易求解, 而在相变点附近, 几乎所有的算法都表现出很差的性能(见图1).

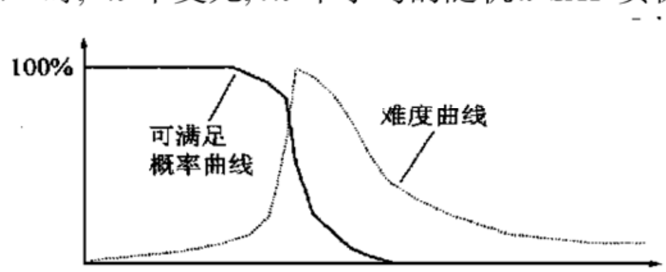

图1 SAT问题的可满足概率和难度曲线图
横轴坐标为子句数/变元数

相变现象是SAT问题的一个重要特性, 通过对这一现象进行研究, 有助于进一步认识SAT问题的性质, 从而设计出更为高效的算法1). 以往, 有很多研究者从解的个数出发, 对SAT问题的相变现象进行研究, 并得到了相变点的一个上界. 但是, 如果只研究解的个数而不考虑赋值之间的相互关系及相互影响, 我们就不可能对相变现象作出一个全面的分析, 因为相变不仅是一个量变的过程, 也是一个质变的过程. 文献[3, 4]分别用完全性算法和不完全算法对SAT问题的求解难度进行了深入的研究, 发现过约束(over-constrained)区域所产生的实例与相变区域所产生的实例相比, 虽然解的个数较少, 但是其求解反而更容易一些. 这就说明, 解的个数并不是决定难度的唯一因素. 由于搜索算法的实质是在赋值空间中寻找解, 因此解的结构也会与搜索的难易程度密切相关[5, 6]. 到目前为止, 还很少有人研究解的结构随 r 的变化情况. 本文通过理论分析, 首先定义了一个描述可满足赋值之间相似程度的结构参数, 即主相似度

1999-01-11收稿, 1999-03-15收修改稿
* 国家自然科学基金重点资助项目(批准号: 69433030)和国家教委博士点基金资助项目

1) Borow D G, Brady M, eds. Special Volume on Frontiers in Problem Solving: Phase Transitions and Complexity. Guest editors: Hogg T, Huberman B A, Williams C P. Artif Intell, 1996, 81(2): 1~15

(定义 6), 然后证明了对于随机 k-SAT 模型($k \geqslant 5$), 当 r 连续增大时, 主相似度将在某个临界点($r = r_{cr}$)发生与可满足概率相变类似的突变现象, 因此也将这种突变现象称为主相似度相变. Borow 等1) 指出, 除了可满足概率2) 和搜索代价, 我们也应该研究其它形式的相变现象, 但至今还尚未见到从理论上证明一般 k-SAT 问题存在某种相变现象的报道.

1　定义和引理

在分析解的结构之前, 首先叙述一些与 SAT 问题相关的定义.

定义 1　合取范式及可满足性(SAT) 问题

(a) 给定一命题变元集 U, 它由 n 个变元 $u_1, \cdots, u_n$ 组成;

(b) t_i: $U \rightarrow \{T, F\}$ 为关于 U 的一个真值赋值($1 \leqslant i \leqslant 2^n$);

(c) 如果 u 是 U 的一个变元, 那么 u 和 $\neg u$ 是 U 的文字, 其中 u 是正文字, $\neg u$ 是负文字, 文字用 L 表示;

(d) 子句是一些文字的析取, 子句用 C 表示;

(e) 合取范式(简称 CNF) 是一些子句的合取, 合取范式用 Λ 表示.

SAT 问题可以定义为: 给定变元集 U 上的合取范式 Λ, 问是否存在一个关于 U 的真值赋值 t, 使得 Λ 为真. 随机 k-SAT 公式的每一个子句都是随机独立产生的, 其过程如下: 从变元集中随机选取 k 个不同的变元, 每个变元在子句中以正文字或负文字形式出现的概率相等.

定义 2　Φ 表示一个函数, 将真值赋值映射为空间中的点, 其定义如下:

$$\Phi(t_i) = X_i(x_{i1}, x_{i2}, \cdots, x_{il}, \cdots, x_{in}), \text{ 其中 } x_{il} = \begin{cases} 1, & t_i(u_l) = \mathrm{T}, \\ 0, & t_i(u_l) = \mathrm{F}. \end{cases}$$

$X_i(x_{i1}, x_{i2}, \cdots, x_{il}, \cdots, x_{in})$ 表示 n 维空间中的一个点, x_{il} 为该点在 l 轴($1 \leqslant l \leqslant n$)上的坐标值.

通过函数 Φ, 每一个赋值都可以唯一对应于空间中的一个点. 例如, 定义在变元集 U 上的 CNF 范式一共有 2^n 个赋值, 分别对应于 n 维空间中的 2^n 个点.

为了研究解的结构, 必须考虑不同赋值之间的相互关系及相互影响. 首先, 我们将赋值组合成赋值对, 并引入相同元数和相似度等概念来表示一个赋值对中两个赋值之间的关系.

定义 3　赋值对: $\langle t_i, t_j \rangle$ 是关于变元集 U 的一个赋值对, 当且仅当 t_i, t_j 是关于变元集 U 的两个真值赋值. 一个赋值对满足 CNF 范式当且仅当该赋值对的两个赋值都满足 CNF 范式. 在本文中, 所讨论的赋值及赋值对均定义在变元集 U 上, 用 A_{pair} 表示所有的赋值对所组成的集合.

注 1　t_i 可以等于 t_j, 即 $\langle t_i, t_i \rangle$ 也是一个赋值对, 当 $t_i \neq t_j$ 时, $\langle t_i, t_j \rangle$ 和 $\langle t_j, t_i \rangle$ 是两个不同的赋值对.

设 $\langle t_i, t_j \rangle$ 是关于变元集 U 的一个赋值对, 根据定义 2 和定义 3, 有

$$\Phi(t_i) = X_i(x_{i1}, x_{i2}, \cdots, x_{il}, \cdots, x_{in}), \quad \Phi(t_j) = X_j(x_{j1}, x_{j2}, \cdots, x_{jl}, \cdots, x_{jn}).$$

定义 4　相同元数 S^f: $A_{\text{pair}} \rightarrow \{0, 1, 2, 3, \cdots\}$,

$$S^f(\langle t_i, t_j \rangle) = \sum_{l=1}^{n} (1 - | x_{il} - x_{jl} |).$$

1) 同 354 页脚注 1)

2) 最近, E. Friedgut 在证明可满足概率相变的存在性问题上取得了很大的进展

一个赋值对的相同元数表示对于该赋值对的两个赋值来说, 其中有多少个变元的赋值相同. 根据定义, 显然有 $0 \leqslant S^f(\langle t_i, t_j \rangle) = S \leqslant n$.

定义 5 相似度 $s^f: A_{\text{pair}} \to \mathrm{R}$,

$$s^f(\langle t_i, t_j \rangle) = \frac{S^f(\langle t_i, t_j \rangle)}{n}.$$

一个赋值对的相似度表示该赋值对的两个赋值相似的程度. 也就是相同元数占变元总数的比例, 函数 s^f 的值 s 越大, 表明两个赋值越相似. 根据定义, 显然有 $0 \leqslant s^f(\langle t_i, t_j \rangle) = s \leqslant 1$.

引入记号, Φ 表示一个随机 k-SAT 公式, 该公式定义在变元集 U 上, 有 rn 个子句. $P(t_i)$ 表示赋值 t_i 满足 Φ 的概率, $P(\langle t_i, t_j \rangle)$ 表示赋值对 $\langle t_i, t_j \rangle$ 满足 Φ 的概率.

首先, 我们知道

$$P(t_i) = \left(1 - \frac{1}{2^k} \right)^{rn}. \tag{1}$$

给定变元总数和子句个数, 赋值对满足 Φ 的概率仅与相同元数有关, 其表达式如下:

$$\text{若 } S^f(\langle t_i, t_j \rangle) = S, \text{则 } P(\langle t_i, t_j \rangle) = \left(\frac{2^k - 2 + \dfrac{S(S-1)\cdots(S-k+1)}{n(n-1)\cdots(n-k+1)}}{2^k} \right)^{rn}. \tag{2}$$

利用定义 4 和定义 5, 并通过阶的分析, 我们可以求出当 n 趋近于无穷大时, $P(\langle t_i, t_j \rangle)$ 的渐近表达式:

$$\text{若 } s^f(\langle t_i, t_j \rangle) = s, \text{ 则 } P(\langle t_i, t_j \rangle) = \sigma(s) \mathrm{e}^{-nrg(s)}(1 + O(1/n)) \text{ 当 } n \to +\infty, \tag{3}$$

其中

$$\sigma(s) = \mathrm{e}^{r\rho(s)}, \ \rho(s) = \frac{k(k-1)}{2(2^k - 2 + s^k)}(s^k - s^{k-1}), \ g(s) = \ln 2^k - \ln(2^k - 2 + s^k).$$

引入记号, A_s 表示相似度为 s 的赋值对所组成的集合.

集合 A_s 的基数

$$|A_s| = 2^n C_n^{ns}. \tag{4}$$

当 n 趋近于无穷大时, 利用 Stirling 公式, 对上式进行渐近分析, 可得

$$|A_s| = \tau(s) \mathrm{e}^{nh(s)}(1 + O(1/n)) \text{ 当 } n \to +\infty, \tag{5}$$

其中, 函数 $\tau(s)$ 和 $h(s)$ 的定义如下:

$$\tau(s) = \begin{cases} 1, & \text{若 } s = 0, 1, \\ \dfrac{1}{\sqrt{2\pi ns(1-s)}}, & \text{若 } 0 < s < 1, \end{cases}$$

$$h(s) = \begin{cases} \ln 2, & \text{若 } s = 0, 1, \\ \ln 2 - s\ln s - (1-s)\ln(1-s), & \text{若 } 0 < s < 1. \end{cases}$$

引入记号, A_s^{Sat} 表示在相似度为 s 的赋值对中, 满足 Φ 的赋值对所组成的集合. 显然, 该集合的基数 $|A_s^{\text{Sat}}|$ 是一个随机变量, $E(|A_s^{\text{Sat}}|)$ 表示该随机变量的期望值.

$$E(|A_s^{\text{Sat}}|) = P(\langle t_i, t_j \rangle) |A_s| = \varphi(s) \mathrm{e}^{nf(s)}(1 + O(1/n)), \text{ 当 } n \to +\infty, \tag{6}$$

其中 $\varphi(s) = \sigma(s)\tau(s)$, $f(s) = h(s) - rg(s)$.

定义 6 主相似度: 给定 r, 若 s_0 满足如下条件: 对于任意的 $0 \leqslant s \leqslant 1$, 有

$$\lim_{n\to+\infty}\frac{\ln E(|A_s^{\mathrm{Sat}}|)-\ln E(|A_{s_0}^{\mathrm{Sat}}|)}{n}\leqslant 0, \tag{7}$$

则 s_0 为主相似度, 本文用 s_{mj}来表示主相似度.

性质 1　给定 r, 若 s_0 满足如下条件: 对于任意的 $0\leqslant s\leqslant 1$, 均存在 $M>0$, 使得当 $n>M$ 时, 有 $E(|A_s^{\mathrm{Sat}}|)\leqslant E(|A_{s_0}^{\mathrm{Sat}}|)$, 则 s_0 是主相似度.

由定义 6 直接得证.

性质 2　给定 r, 若 s_0 不是主相似度, 则存在 $\delta>0$ 和 $M>0$, 使得当 $n>M$ 时, 有 $E(|A_{s_{\mathrm{mj}}}^{\mathrm{Sat}}|)\geqslant \mathrm{e}^{n\delta}E(|A_{s_0}^{\mathrm{Sat}}|)$.

由定义 6 及表达式(6)式直接得证.

从性质 1 和性质 2 可以看出, 当 n 充分大以后, 使 $E(|A_s^{\mathrm{Sat}}|)$取最大值的相似度一定是主相似度, $E(|A_{s_{\mathrm{mj}}}^{\mathrm{Sat}}|)$ 比 $E(|A_{s_0}^{\mathrm{Sat}}|)$($s_0$不是主相似度)大 n 的指数倍. 因此, 主相似度的大小代表了可满足赋值之间的相似程度, 主相似度的值越大, 表明可满足赋值之间越相似.

引理 1　s_0 为主相似度当且仅当 s_0 使函数$f(s)$取最大值.

由定义 6 及表达式(6)式直接得证.

根据引理 1, s_0 为主相似度当且仅当 s_0 使函数$f(s)$取最大值, 函数$f(s)$的极值点应满足如下条件:

$$f'(s)=h'(s)-rg'(s)=-\ln s+\ln(1-s)+r\frac{ks^{k-1}}{2^k-2+s^k}=0, \tag{8}$$

$$\Leftrightarrow r(s)=\frac{h'(s)}{g'(s)}=\frac{1}{k}\left|\frac{2^k-2}{s^{k-1}}+s\right|(\ln s-\ln(1-s)). \tag{9}$$

上式给出了 r 与极值点之间的函数关系, 通过对该函数的性质进行研究, 就可以得到 r 与最大值点之间的关系, 从而获得主相似度随 r 的变化规律. 为了对函数 $r(s)$的性质进行研究, 首先来分析它的导函数的性质.

引理 2　给定子句长度 $k(k\geqslant 5)$, $r''(s)=0$ 在区间[0.5, 1)上有且仅有一个解 s_{02}, 当 $s<s_{02}$时, $r''(s)<0$; 当 $s>s_{02}$时, $r''(s)>0$.

证　$r(s)$的二阶导函数 $r''(s)$的表达式如下:

$$r''(s)=F(s)\frac{2^k-2}{s^{k+1}(1-s)^2},$$

其中

$$F_1(s)=k(k-1)(\ln s-\ln(1-s))(1-s)^2-2(k-1)(1-s)+2s-1,$$

$$F(s)=F_1(s)+\frac{s^k}{2^k-2},\ F(0.5)<0,\ \lim_{s\to 1}F(s)>0.$$

$F(s)$在区间[0.5, 1)上是连续函数, 根据介值定理及上式, 至少存在一个点 s_{02}, 使得 $F(s_{02})=0$. 下面证明最多也只有一个零点, 分以下两种情况讨论:

情形 1　如果 $F'_1(s)=0$ 在区间[0.5, 1)上无解, 可以证明 $F'(s)>0$, 即 $F(s)$在区间[0.5, 1)上是单调递增函数, 故只有一个零点;

情形 2　如果 $F'_1(s_0)=0$, 可证 $F_1(s_0)>0$, 即 $F_1(s)$在极值点处的取值均大于零, 同样可以证明 $F(s)$在区间[0.5, 1)上只有一个零点.

由于 $F(s)$ 与 $r''(s)$ 的符号特性完全一样, 故引理 2 成立.

引理 3 给定子句长度 $k(k \geqslant 5)$, $r'(s)=0$ 在区间 $[0.5, 1)$ 上有且仅有两个解 s_{01} 和 s_{03} $(s_{01}< s_{02}< s_{03})$, 当 $0.5 \leqslant s< s_{01}$ 时, $r'(s)>0$; 当 $s_{01}< s< s_{03}$ 时, $r'(s)<0$; 当 $s_{03}< s< 1$ 时, $r'(s)>0$.

证

$$r'(s)\ \frac{ks^k}{(k-1)(2^k-2)-s^k} \leqslant (\ln s - \ln(1-s)) + \frac{2^k-1}{(k-1)(2^k-2)-1}\ \frac{1}{(1-s)},$$

令

$$a=\frac{2^k-1}{(k-1)(2^k-2)-1},\ H(s)=\frac{a}{1-s}-(\ln s-\ln(1-s)).$$

当 $k \geqslant 5$ 时, $0.5<\frac{1}{1+a}<1$, 可以证明 $H\left|\frac{1}{1+a}\right|<0$, $r'\left|\frac{1}{1+a}\right|<0$. 根据引理 2, s_{02} 是函数 $r'(s)$ 的最小值点, 因此当 $k \geqslant 5$ 时, $r'(s_{02})<0$.

由 $r'(s)$ 的表达式, 可得 $r'(0.5)>0$, $\lim_{s \to 1} r'(s)=+\infty$.

根据引理 2, 在区间 $[0.5, s_{02})$ 上, $r'(s)$ 是连续减函数, 因此存在 s_{01}, 使得 $r'(s_{01})=0$, 当 $0.5 \leqslant s< s_{01}$ 时, $r'(s)>0$, 当 $s_{01}< s \leqslant s_{02}$ 时, $r'(s)<0$; 在区间 $(s_{02}, 1)$ 上, $r'(s)$ 是连续增函数, 因此存在 s_{03}, 使得 $r'(s_{03})=0$, 当 $s_{02} \leqslant s< s_{03}$ 时, $r'(s)<0$, 当 $s_{03}< s< 1$ 时, $r'(s)>0$. 故引理 3 成立.

通过引理 3, 很容易推出函数 $r(s)$ 的增减性质: 当 $0.5 \leqslant s \leqslant s_{01}$ 时, $r(s)$ 是单调增函数; 当 $s_{01} \leqslant s \leqslant s_{03}$ 时, $r(s)$ 是单调减函数; 当 $s_{03} \leqslant s< 1$ 时, $r(s)$ 是单调增函数. 因此, 我们可以定义 $r(s)$ 在各区间上的反函数, 其具体定义如下:

$$s_1(r)=r^{-1}(s):\ [0, r(s_{01})] \to [0.5,\ s_{01}];$$

$$s_2(r)=r^{-1}(s):\ [r(s_{03}),\ r(s_{01})] \to [s_{01},\ s_{03}];$$

$$s_3(r)=r^{-1}(s):\ [r(s_{03}),\ +\infty) \to [s_{03},\ 1).$$

首先分析当 $r< r(s_{03})$ 或 $r> r(s_{01})$ 时, 主相似度的变化情况, 由(8)、(9)式可得

$$f'(s)=h'(s)-rg'(s)=g'(s)\left|\frac{h'(s)}{g'(s)}-r\right|,$$

$$g'(s)=-\frac{ks^{k-1}}{2^k-2+s^k}<0. \qquad (10)$$

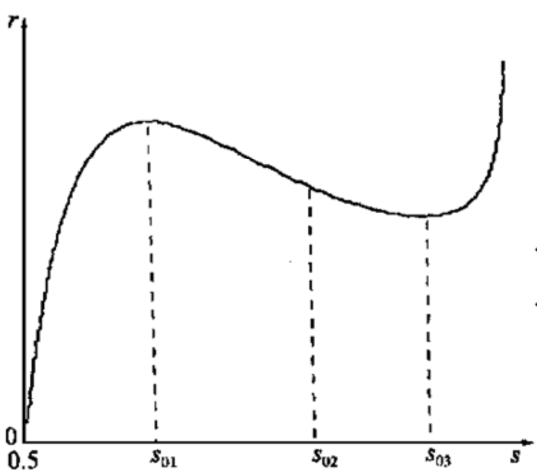

图 2 随机 k-SAT 模型$(k \geqslant 5)$ 的 $r(s)$ 函数曲线

给定 r, 根据图 2 及(10)式, 当 $r< r(s_{03})$ 时, 函数 $f(s)$ 有唯一的极值点 $s_1(r)$, 在区间 $[0.5, s_1(r))$ 上, $f'(s)>0$, 在区间 $(s_1(r), 1)$ 上, $f'(s)<0$, 故 $s_1(r)$ 使函数 $f(s)$ 取最大值, 因此由引理 1 可得, 当 $r< r(s_{03})$ 时, $s_1(r)$ 是主相似度. 同理可知, 当 $r> r(s_{01})$ 时, $s_3(r)$ 是主相似度. 由于 $s_1(r)$ 和 $s_3(r)$ 均为连续增函数, 因此当 $r< r(s_{03})$ 或 $r> r(s_{01})$ 时, 随着 r 的连续增加, 主相似度也将连续增大. 但下一节的定理将证实: 当 $r(s_{03}) \leqslant r \leqslant r(s_{01})$ 时, 主相似度的变化曲线在某个临界点处不

连续.

2　主相似度相变的存在性定理

本节将证明: 当 r 在区间 $[r(s_{03}),\ r(s_{01})]$ 上连续增加时, 主相似度会发生与可满足概率相变类似的突变现象(见图 3), 即是, 存在某个临界值 r_{cr}, 当 r 跨过该临界点时, 主相似度从一个较小的值突然变为一个较大的值, 本文将这种突变现象称为主相似度相变. 下面, 我们就来证明主相似度相变的存在性定理.

定理 1　对于随机 k-SAT 模型, 给定子句长度 $k(k\geqslant 5)$, 存在某个临界值 r_{cr}(临界值 r_{cr} 的大小与 k 有关), 使得对于任意小的正值 ε, 当 $r=r_{cr}-\varepsilon$ 时, $s_{mj}<s_{1cr}$, $\lim\limits_{r\to r_{cr}-0}s_{mj}=s_{1cr}$; 当 $r=r_{cr}+\varepsilon$ 时, $s_{mj}>s_{3cr}$, $\lim\limits_{r\to r_{cr}+0}s_{mj}=s_{3cr}$, 其中 $s_{1cr}<s_{3cr}$.

证　给定 r, 当 $r(s_{03})<r<r(s_{01})$ 时, 函数 $f(s)$ 有 3 个极值点, 分别是 $s_1(r)$、$s_2(r)$ 和 $s_3(r)$. 同样, 根据(10)式, 很容易判断出 $s_1(r)$ 和 $s_3(r)$ 是极大值点, $s_2(r)$ 是极小值点. 通过对两个极大值进行比较, 即可求得主相似度, 因此首先定义如下函数:

$$F(r)=f(s_1(r))-f(s_3(r)),\quad r(s_{03})\leqslant r\leqslant r(s_{01}).\tag{11}$$

根据图 2 及(10)式, 当 $r=r(s_{03})$ 时, $s_1(r(s_{03}))$ 是 $f(s)$ 唯一的最大值点, 因此有

$$F(r(s_{03}))=f(s_1(r(s_{03})))-f(s_3(r(s_{03})))>0.\tag{12}$$

同理, 当 $r=r(s_{01})$ 时, $s_3(r(s_{01}))$ 是 $f(s)$ 唯一的最大值点, 因此有

$$F(r(s_{01}))=f(s_1(r(s_{01})))-f(s_3(r(s_{01})))<0.\tag{13}$$

对函数 $F(r)$ 求导, 可得

$$\begin{aligned}F'(r)=&\ h'(s_1(r))s'_1(r)-g(s_1(r))-rg'(s_1(r))s'_1(r)-\\&\ h'(s_3(r))s'_3(r)+g(s_3(r))+rg'(s_3(r))s'_3(r).\end{aligned}\tag{14}$$

对上式进行化简, 并利用 $s_1(r)$ 和 $s_3(r)$ 满足极值方程, 即

$$\begin{aligned}&h'(s_1(r))-rg'(s_1(r))=0,\\&h'(s_3(r))-rg'(s_3(r))=0.\end{aligned}\tag{15}$$

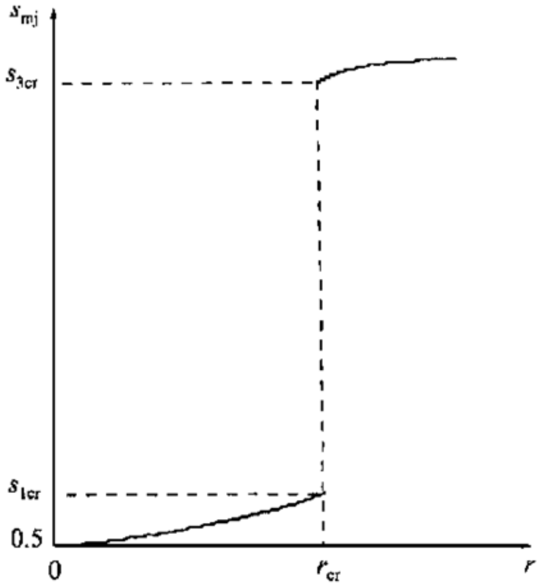

图 3 随机 k-SAT 模型($k\geqslant 5$)的主相似度随 r 的变化曲线

s_{mj} 在 $r=r_{cr}$ 处发生了相变现象

将(15)式代入(14)式, 可得

$$F'(r)=\ln(2^k-2+(s_1(r))^k)-\ln(2^k-2+(s_3(r))^k).\tag{16}$$

显然 $s_1(r)\leqslant s_{01}<s_{03}\leqslant s_3(r)$, 因此有

$$F'(r)<0.\tag{17}$$

根据介值定理及(12)、(13)和(17)式, $F(r)$ 存在唯一的零点 r_{cr}, 并有如下事实成立:

当 $r(s_{03})\leqslant r<r_{cr}$ 时, $f(s_1(r))>f(s_3(r))$, 可得 $s_{mj}=s_1(r)<s_1(r_{cr})$;

当 $r_{cr}<r\leqslant r(s_{01})$ 时, $f(s_1(r))<f(s_3(r))$, 可得 $s_{mj}=s_3(r)>s_3(r_{cr})$;

令 $s_{1cr}=s_1(r_{cr})$, $s_{3cr}=s_3(r_{cr})$, 显然, $s_{1cr}<s_{3cr}$,

当 $r=r_{cr}$时, $f(s_{1cr})=f(s_{3cr})$, 即 s_{1cr}和 s_{3cr}都是最大值点, 故 $s_{mj}=s_{1cr}$, s_{3cr}. $s_1(r)$和 $s_3(r)$均为连续增函数, 因此有

当 $r=r_{cr}-\varepsilon$时, $s_{mj}<s_{1cr}$, $\lim_{r\to r_{cr}-0}s_{mj}=s_{1cr}$; 当 $r=r_{cr}+\varepsilon$时, $s_{mj}>s_{3cr}$, $\lim_{r\to r_{cr}+0}s_{mj}=s_{3cr}$.

综上所述, 定理 1 成立.

3 结论

从定理 1 可以看出, 主相似度确实发生了相变现象, 当 r 跨过临界点$r=r_{cr}$时, 主相似度从一个较小的值 s_{1cr}突然跳变到一个较大的值 s_{3cr}. 根据本文的定义, 主相似度是一个与解的结构有关的参数, 其大小代表了可满足赋值之间的相似程度, 主相似度的值越大, 表明可满足赋值之间越相似. 因此, 这种相变现象可以描述为: 当 r 连续增加, 到达某一个临界点时($r=r_{cr}$), 解的结构将发生相变现象, 可满足赋值之间的关系突然由差别较大变得很相似.

本文的研究表明, 除了可满足概率相变以外, SAT 问题也确实还存在其它形式的相变现象. 这一点与自然界中的许多相变现象类似, 即伴随着某种相变的发生, 往往会出现一些其它的突变现象, 虽然这些现象的表现形式各异, 但它们之间有着密切的联系, 通常从不同的侧面反映出事物变化的本质. 因此, 我们也应该从不同的角度出发来分析 SAT 问题的相变现象, 从而更好地认识 SAT 问题的性质. 由于至今还尚未见到证明一般 k-SAT 问题存在某种相变现象的报道, 所以本文的工作将会对这方面的研究有一定的促进作用.

致谢 在论文写作过程中, 与梁东敏、栾尚敏和黄雄等进行过有启发性的讨论, 特致谢意.

参 考 文 献

1 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, (11): 1 208~ 1 217

2 Gent I P, Walsh T. The SAT phase transition. In: Proc of ECAI-94, 105~ 109

3 Selman B, Kirkpatrick S. Critical behavior in the computational cost of satisfiability testing. Artif Intell, 1996, 81: 273~ 295

4 Clark D A, Frank J, Gent I P, et al. Local search and the number of solutions. In: Proc of CP-96. Lecture Notes in Computer Science, Vol 1118. Berlin: Springer, 1996. 119~ 133

5 Dubois O, Boufkhad Y. A general upper bound for the satisfiability threshold of random r-SAT formulae. Journal of Algorithms, 1997, 24: 395~ 420

6 Kirousis L M, Kranakis E, Krizanc D, et al. Approximating the unsatisfiability threshold of random formulas. Random Structures and Algorithms, 1998, 12: 253~ 269