文章编号: 1008-1542(2006) 02-0122-04

有限域上特征为奇数的正交空间中一类 Cartesian认证码的构作

李丽军[1], 李增提[2]

(1. 河北政法职业学院计算机系, 河北石家庄 050061; 2. 廊坊师范学院数学系, 河北廊坊 065000)

摘 要: 利用有限域上特征为奇数的正交几何构造了一类 Cartesian认证码, 并且计算了其参数及模仿攻击成功的概率 P_I 和替换攻击成功的概率 P_S, 这类 Cartesian认证码对 P_I 是最优的。

关键词: 有限域; 特征为奇数的正交几何; 认证码

中图分类号: O157. 4 文献标识码: A

A construction of Cartesian authentication code from odd characteristic orthogonal geometry

LI Li-jun[1], LI Zeng-ti[2]

(1. Computer Science Department, Hebei Professional College of Political Sciences and Law, Shijiazhuang Hebei 050061, China; 2. Department of Mathematics, Langfang Normal College, Langfang Hebei 065000, China)

Abstract: A construction of Cartesian authentication code from odd characteristic orthogonal geometry is given. Its size parameters and its probabilities of successful impersonation attack P_I and of successful substitution attack P_S, are computed respectively, and this Cartesian authentication code is the best to P_I.

Key words: finite field; odd characteristic orthogonal geometry; authentication code

设 S, E 和 M 是 3个非空有限集, $f: S\times E\to M$ 是 1个映射, 且满足下面的条件:

1)映射 f 是满射;

2)对任给的 $m\in M$ 和 $e\in E$, 如果存在 1个 $s\in S$, 使得 $f(s, e)=m$, 这样的 s 是被 m 和 e 所唯一确定的, 则称四元组 $(S, E, M; f)$ 是 1个认证码。

假设 $(S, E, M; f)$ 是 1个认证码, S, E 和 M 分别称为信源集、编码规则集和信息集, f 称为编码映射。对 $s\in S$, $e\in E$, $m\in M$, 或 $m=f(s, e)$, 则称信源 s 在编码规则 e 下加密成信息 m, 或简单地说 m 包含编码规则 e, 也说 s 是相应于信息 m 的信源, 基数 $|S|$, $|E|$ 和 $|M|$ 称为这个码的参数。假如认证码 $(S, E, M; f)$ 还满足: 对于任意的 $m\in M$, 总存在唯一的信源 s, 使得 $m=f(s, e)$, 其中 e 是包含在 m 中的任一编码规则, 则称这样的认证码为 Cartesian认证码。对于 1个 Cartesian认证码, 若 $P_I=|S|/|M|$, 则称 P_I 是最优的。

利用有限域上的典型群几何构造认证码, 在文献[1~5]中已得到了一些重要成果。在本文中, 笔者利用有限域上特征为奇数的正交空间构造了一类 Cartesian认证码, 且是一类 P_I 最优认证码, 并计算了其参数。

1 预备知识

设 F_q 是 q 元有限域, q 是 1个素数的幂。令 Z 是 F_q^* 中 1个取定的非平方元。设 $n=2v+\delta$, 其中 v 是

收稿日期: 2005-11-30; 修回日期: 2006-03-27; 责任编辑: 王士忠

作者简介: 李丽军(1967-), 女, 河北衡水人, 副教授, 硕士, 主要从事基础数学和计算机应用方面的研究。

非负整数, δ= 0, 1或 δ= 2。引进符号:

$$\Delta=\begin{cases}\cong, & \text{if } \delta=0,\\ (1)\text{or}(Z), & \text{if } \delta=1,\\ \begin{pmatrix}1 & \\ & -Z\end{pmatrix}, & \text{if } \delta=2,\end{cases}\quad \text{并且令 } S_{2v+\delta}=\begin{pmatrix}0 & I^{(v)} & \\ I^{(v)} & 0 & \\ & & \Delta\end{pmatrix},$$

则有限域 F_q 上满足 $TS_{2v+\delta}T^{\mathrm{T}}\equiv S_{2v+\delta}$的矩阵 T 的集合关于矩阵的乘法构成 F_q 上的 $2v+\delta$阶正交群, 记作 $O_{2v+\delta,\Delta}(F_q)$, 即 $O_{2v+\delta,\Delta}(F_q)=\{T\in GL_{2v+\delta}(F_q)\mid TS_{2v+\delta}T^{\mathrm{T}}\equiv S_{2v+\delta}\}$。

群 $O_{2v+\delta,\Delta}(F_q)$在 $F_q^{(2v+\delta)}$ 上有如下一个作用:

$F_q^{(2v+\delta)}\times O_{2v+\delta,\Delta}(F_q)\to F_q^{(2v+\delta)}$, $((x_1, x_2, \cdots, x_{2v+\delta}), T)\to (x_1, x_2, \cdots, x_{2v+\delta})T$。

带有如上群 $O_{2v+\delta,\Delta}(F_q)$作用的向量空间叫做 F_q 上关于 $S_{2v+\delta}$的 $2v+\delta$维正交空间。

设 P 是 $F_q^{(2v+\delta)}$ 的 1个子空间, 用 $P^{\perp}$表示子空间 P的对偶空间, 即

$$P^{\perp}=\{x\in F_q^{(2v+\delta)}\mid xS_{2v+\delta}y^{\mathrm{T}}=0,\ \forall y\in P\},$$

当 δ= 2时, $(m, 2s+\gamma, s, \ )$型子空间存在, 当且仅当 $2s+\gamma\leqslant m\leqslant v+s+\min(2, \gamma)$;

当 δ= 2时, 存在 $(m, 2s+\gamma, s, \ )$型子空间包含 $(m_1, 2s_1+\gamma_1, s_1, \Gamma_1)$型子空间, 当且仅当

$$2s+\gamma\leqslant m\leqslant v+s+\min\{2, \gamma\},\ 2s_1+\gamma_1\leqslant m_1\leqslant v+s_1+\min\{2, \gamma_1\},$$

$$2m-2m_1\geqslant(2s+\gamma)-(2s_1+\gamma_1)+|\gamma-\gamma_1|\geqslant 2|\gamma-\gamma_1|。$$

用 $N(m, 2s+\gamma, s, \Gamma; 2v+2)$表示 $2v+2$维正交空间 $F_q^{(2v+2)}$ 中关于 S_{2v+2}的 $(m, 2s+\gamma, s, \Gamma)$型子空间的个数, 则

$$N(m, 2s+\gamma, s, \Gamma; 2v+2)=$$

$$q^{2s(v+s-m)+s(\gamma+2)-\gamma(m-2s-\gamma)}\frac{\prod_{i=v+s-m+\gamma+1}^{v}(q^i-1)(q^{i+1}+1)}{\prod_{i=1}^{s}(q^i-1)\prod_{i=0}^{s+\gamma-1}(q^i+1)\prod_{i=1}^{m-2s-\gamma}(q^i-1)}n_0(m, 2s+\gamma, s, \Gamma; 2v+2),\qquad (1)$$

其中: $n_0(m, 2s, s, 2v+2)=1$;

$n_0(m, 2s+1, s, \Gamma; 2v+2)=q^{v-s}(q^{v+s-m+2}+1)$;

$n_0(m, 2s+2, s, 2v+2)=q^{2(v-s)}(q^{v+s-m+2}+1)(q^{v+s-m+3}+1)$。

2 主要结果

定理 **1**　设 $1\leqslant m_0\leqslant v$, $m_0+2s+2\leqslant m\leqslant v+s+1$, 在特征为奇数的正交空间 $F_q^{(2v+2)}$ 上, P_0 是 1个固定的 $(m_0, 0, 0)$型子空间, 信源集 S 是包含 P_0 且与 P_0 正交的 $(m, 2s+1, s, \Gamma)$型子空间集, 编码规则集 E 是包含 P_0 的 $(m_0+1, 2, 1)$型子空间集, 信息集 M 是包含 P_0 且与 P_0 不正交的 $(m+1, 2(s+1)+1, s+1, \Gamma)$型子空间集, 任给 $s\in S$, $e\in E$, $f(s, e)=s+e$, 那么如上构作的 $(S, E, M; f)$是 1个 Cartesian认证码。

证　明　设 s是 1个信源, 即是 1个包含 P_0 且与 P_0 正交的 $(m, 2s+1, s, \Gamma)$型子空间 Q, 假设

$$Q=\begin{pmatrix}Q_0\\ P_0\end{pmatrix}_{m_0}^{m-m_0},\quad \text{且}\quad QS_{2v+2}Q^{\mathrm{T}}=\begin{pmatrix}0 & I^{(s)} & & \\ I^{(s)} & 0 & & \\ & & \Gamma & \\ & & & 0^{(m-2s-1)}\end{pmatrix};$$

设 e是 1个编码规则, 即是 1个包含 P_0 的 $(m_0+1, 2, 1)$型子空间 R, 设

$$R=\begin{pmatrix}P_0\\ u\end{pmatrix},\quad \text{且}\quad RS_{2v+2}R^{\mathrm{T}}=\begin{pmatrix}0^{(m_0-1)} & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix};$$

显然 $u\notin Q$, 故 $Q+\langle u\rangle$是 1个 $m+1$维子空间, 又因

$$\begin{pmatrix} Q \\ u \end{pmatrix} S_{2v+2} \begin{pmatrix} Q \\ u \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 0 & I^{(s)} & 0 & 0 & 0 & 0 & * \\ I^{(s)} & 0 & 0 & 0 & 0 & 0 & * \\ 0 & 0 & \Gamma & 0 & 0 & 0 & * \\ 0 & 0 & 0 & 0^{(m-m_0-2s-1)} & 0 & 0 & * \\ 0 & 0 & 0 & 0 & 0^{(m_0-1)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ * & * & * & * & 0 & 1 & * \end{pmatrix},$$

于是 $P = Q + \langle u \rangle$与 P_0 不正交, 所以 $P = Q + \langle u \rangle$是 1个 $(m+1, 2(s+1)+1, s+1, \Gamma)$型子空间, 即 P 为 1个信息, f 为 1个映射 (* 表示计算后应得值)。

现设 m 是 1个信息, 即 m 是 1个包含 P_0 且与 P_0 不正交的 $(m+1, 2(s+1)+1, s+1, \Gamma)$型子空间 P, 不妨设

$$P = \begin{pmatrix} Q_0 \\ P_0 \\ u \end{pmatrix} \begin{matrix} m-m_0 \\ m_0 \\ 1 \end{matrix}, \text{且} \quad \begin{pmatrix} Q \\ u \end{pmatrix} S_{2v+2} \begin{pmatrix} Q \\ u \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 0 & I^{(s)} & 0 & 0 & 0 & 0 & 0 \\ I^{(s)} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \Gamma & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0^{(m-m_0-2s-1)} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0^{(m_0-1)} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

那么 $Q = Q_0 + P_0$ 是 1个 $(m, 2s+1, s, \Gamma)$型子空间且 P_0 与 Q 正交, $R = P_0 + \langle u \rangle$是 1个 $(m_0+1, 2, 1)$型子空间, 所以 Q 是 1个信源, R 是 1个编码规则且 $P = Q + R$, 即 f 是 1个满射。

设 Q'是相应于 P 的另一个信源, 记 $P = Q' + R'$, 对某个编码规则 R', 任意的 $x \in Q'$, 设 $x = w_1 + w_2 + \lambda u$, $w_1 \in Q_0$, $w_2 \in P_0$, 由于 Q'正交于 P_0, 因此 $P_0 S_{2v+2} x^{\mathrm{T}} = 0$, 于是 $P_0 S_{2v+2} (w_1^{\mathrm{T}} + w_2^{\mathrm{T}} + \lambda u^{\mathrm{T}}) = 0$。

由 $P_0 S_{2v+2} w_1^{\mathrm{T}} = 0$, $P_0 S_{2v+2} w_2^{\mathrm{T}} = 0$, $P_0 S_{2v+2} u^{\mathrm{T}} \neq 0$, 得 $\lambda = 0$, 于是 $x = w_1 + w_2$, $w_1 \in Q_0$, $w_2 \in P_0$, 即 $x = w_1 + w_2 \in Q$, 故 $Q' \subset Q$, 又因 $\dim Q = \dim Q' = m$, 所以 $Q = Q'$, 因此以上构作是 1个 Cartesian认证码。

引理 **1** $|S| = N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)$。

证 明 由于特征为奇数的正交群 $O_{2v+2\Delta}(F_q)$可迁地作用在同类型的子空间集合上, 其中

$$\Delta = \begin{pmatrix} 1 & 0 \\ 0 & -Z \end{pmatrix}, \text{不妨设} \quad P_0 = \begin{matrix} m_0 \end{matrix} \begin{matrix} m_0 & v-m_0 & m_0 & v-m_0 & 2 \end{matrix} \\ (I \quad 0 \quad 0 \quad 0 \quad 0), \quad Q = \begin{matrix} m_0 \\ m-m_0 \end{matrix} \begin{matrix} m_0 & v-m_0 & m_0 & v-m_0 & 2 \end{matrix} \\ \begin{pmatrix} I & 0 & 0 & 0 & 0 \\ 0 & Q_1 & 0 & Q_2 & Q_3 \end{pmatrix};$$

由于 $QS_{2v+2}Q^{\mathrm{T}} = \begin{matrix} m_0 \\ m-m_0 \end{matrix} \begin{matrix} m_0 & m-m_0 \end{matrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & Q_1 Q_2^{\mathrm{T}} + Q_2 Q_1^{\mathrm{T}} + Q_3 \Delta Q_3^{\mathrm{T}} \end{pmatrix}$ 合同于 $M(m, 2s+1, s, \Gamma)$, 于是

$$(Q_1 \quad Q_2 \quad Q_3) \begin{pmatrix} 0 & I^{(v-m_0)} & 0 \\ I^{(v-m_0)} & 0 & 0 \\ 0 & 0 & \Delta \end{pmatrix} \begin{pmatrix} Q_1^{\mathrm{T}} \\ Q_2^{\mathrm{T}} \\ Q_3^{\mathrm{T}} \end{pmatrix} = Q_1 Q_2^{\mathrm{T}} + Q_2 Q_1^{\mathrm{T}} + Q_3 \Delta Q_3^{\mathrm{T}},$$

合同于 $M(m-m_0, 2s+1, s, \Gamma)$。因此, $(Q_1 \quad Q_2 \quad Q_3)$是 $F_q^{2(v-m_0)+2}$ 上的 1个 $(m-m_0, 2s+1, s, \Gamma)$型子空间, 所以 $|S| = N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)$。

引理 **2** $|E| = q^{2(v-m_0)+2}$。

证 明 由于特征为奇数的正交群 $O_{2v+2\Delta}(F_q)$可迁地作用在同类型子空间的集合上, 不妨设

$$P_0 = \begin{matrix} m_0 & v-m_0 & m_0 & v-m_0 & 2 \end{matrix} \\ (I \quad 0 \quad 0 \quad 0 \quad 0),$$

由 $P_0 S_{2v+2} u^{\mathrm{T}} = (0, \cdots, 0, 1)^{\mathrm{T}}$ 有

$$R=\begin{array}{c} \begin{matrix} m_0 & v-m_0 & m_0 & v-m_0 & 2 \end{matrix} \\ \begin{pmatrix} I & 0 & 0 & 0 & 0 \\ 0 & u_1 & u_2 & u_3 & u_4 \end{pmatrix} \begin{matrix} m_0 \\ 1 \end{matrix} \end{array},$$

其中 u_1, u_3, u_4 是任意的向量, $u_2=(0, \cdots, 0, 1)$, 于是 $|E|=q^{2(v-m_0)+2}$。

引理 **3**　包含在 1个信息中的编码规则的个数是 q^{m-m_0}。

证　明　设 P 是 1个信息, Q 是包含在 P 中的 1个信源, $R=P_0+\langle u\rangle$是包含在 P 中的 1个编码规则, 那么, $P=Q+R$。设 Q_0 是 P_0 在 Q 中的 1个补子空间, 则 $P=Q_0\dot{+}P_0\dot{+}\langle u\rangle$, 于是包含在 P 中的 1个 $(m_0+1, 2, 1)$型子空间具有形式 $P_0+\langle w+u\rangle$, $w\in Q_0$。这是因为

$$\begin{pmatrix} P_0 \\ w+u \end{pmatrix} S_{2v+2} \begin{pmatrix} P_0 \\ w+u \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 0^{(m_0-1)} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & * \end{pmatrix},$$

又 $\dim Q_0=m-m_0$, 所以包含在 P 中的编码规则 R 的个数为 q^{m-m_0}。

引理 **4**　$|M|=q^{2v-m-m_0+2}N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)$。

证　明　由于每个信息包含唯一的信源, 而每个信息包含 q^{m-m_0}个编码规则, 故

$$|M|=|S||E|/q^{m-m_0},$$

$$|M|=q^{2(v-m_0)+2}N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)/q^{m-m_0},$$

$$|M|=q^{2v-m-m_0+2}N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)。$$

引理 **5**　设 P_1, P_2 为 2个信息, Q_1, Q_2 是相应于 P_1, P_2 的信源, 设 $Q_1\cap Q_2=Q_0$, $\dim Q_0=r$, 那么包含在 P_1, P_2 中的编码规则的个数为 q^{r-m_0}, 其中 $m_0\leqslant r\leqslant m-1$。

证　明　从 $P_0\subset Q_1$, $P_0\subset Q_2$ 得 $P_0\subset Q_1\cap Q_2$, 故 $r\geqslant m_0$; 因 $P_1\neq P_2$, 得 $Q_1\neq Q_2$; 于是 $r\leqslant m-1$, 所以 $m_0\leqslant r\leqslant m-1$。

设 $P_0+\langle u\rangle$是包含在 P_1 和 P_2 中的编码规则, 那么　$P_1=Q_1+\langle u\rangle$, $P_2=Q_2+\langle u\rangle$。

设 $Q_0=P_0\dot{+}Q_0'$, $Q_1=Q_1'\dot{+}Q_0$, $Q_2=Q_2'\dot{+}Q_0$, 则　$P_1=P_0\dot{+}Q_0'\dot{+}Q_1'\dot{+}\langle u\rangle$, $P_2=P_0\dot{+}Q_0'\dot{+}Q_2'\dot{+}\langle u\rangle$, 于是同时包含在 P_1, P_2 中的编码规则 R 的形式为　$R=P_0+\langle u+v\rangle$, 其中 $v\in Q_0'$。

反之, 设 R'是同时包含在 P_1, P_2 中的 1个编码规则, 令 $x\in R'$, 则

$$x=v_0+v_1+v_1'+\mu_1 u=v_0'+v_2+v_2'+\mu_2 u;\ v_0, v_0'\in P_0;\ v_1, v_2\in Q_0';\ v_1'\in Q_1';\ v_2'\in Q_2'。$$

由 $\mu_1 P_0 S_{2v+2} u^{\mathrm{T}}=\mu_2 P_0 S_{2v+2} u^{\mathrm{T}}$ 及 $P_0 S_{2v+2} u^{\mathrm{T}}\neq 0$ 得 $\mu_1=\mu_2$, 于是有

$$v_0+v_1+v_1'=v_0'+v_2+v_2'\in Q_1\cap Q_2=Q_0。$$

故 $v_1'=v_2'=0$。因 $Q_0=P_0\dot{+}Q_0'$, 所以由 $v_0+v_1=v_0'+v_2$ 得 $v_0=v_0'$, $v_1=v_2$, 因此 R 的形式为

$$R=P_0+\langle u+v\rangle, \text{其中 } v\in Q_0'。$$

因 $\dim Q_0'=r-m_0$, 故 R 的个数为 q^{r-m_0}。

由以上引理得

$$P_I=q^{m-m_0}/q^{2(v-m_0)+2}=1/q^{2v-m-m_0+2}=|S|/|M|, P_S=\max_{m_0\leqslant r\leqslant m-1} q^{r-m_0}/q^{m-m_0}=\max_{m_0\leqslant r\leqslant m-1} 1/q^{m-r},$$

于是 P_I 是最优的。由于给 1个信息 P_1, 总存在 1个信息 P_2, 使这 2个信息对应的 2个信源 Q_1 与 Q_2 交的维数为 $m-1$, 因此, $P_S=1/q$。

综上所述, 有

定理 **2**　以上构作得到 1个 Cartesian认证码, 其参数分别为

$$|S|=N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2), |E|=q^{2(v-m_0)+2},$$

$$|M|=q^{2v-m-m_0+2}N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)。$$

成功的攻击概率分别为

$$P_I=1/q^{2v-m-m_0+2}, P_S=1/q。$$

(下转第 180页)

机制。双层基于案例推理机制的设计深化了基于案例推理的研究,扩展了其局限性,为其以后的进一步发展奠定了一定的基础。

参考文献:

[1] WASTON I. Case-based reasoning is a methodology not a technology[J]. Knowledge Based System, 1999, (12): 303-308.
[2] STANFILL C. Learning to read: Memory-based model[A]. Proceedings of the DARPA Workshop on Case-based Reasoning[C]. Calif: San Mateo, 1989.
[3] HAMMOND K. Case-based Planning: Viewing Planning as Memory Task[M]. New York: Academic, 1989.
[4] BRANTING L. Integrating generalizations with exemplar-based reasoning[A]. Proceedings of the DARPA Workshop on Case-based Reasoning[C]. Calif: San Mateo, 1989.
[5] SELFRIDGE M, CUTHILL B. Retrieving relevant out-of-context cases: Dynamic memory approach to case-based reasoning[A]. Proceedings of the Workshop on Case-based Reasoning[C]. Calif: San Mateo, 1989.
[6] TURNER R. Organizing and using schematic knowledge for medical diagnosis[A]. Proceedings of the DARPA Workshop on Case-based Reasoning[C]. Calif: San Mateo, 1989.
[7] 严 浩,陆正军,王 岚. 基于面向对象技术的软件代理模型研究[J]. 河北科技大学学报, 2001, 22(4): 62-64.
[8] 李国昌,李 志. 智能决策支持系统知识库体系结构的研究[J]. 河北科技大学学报, 2002, 23(1): 48-50.
[9] WATSON I, MARIR F. Case-based reasoning review[J]. The Knowledge Engineering Review, 1994, 9(5): 355-381.
[10] SHIU S, YEUNG D, SUN C, et al. Transferring case knowledge to adaptation knowledge: An approach for case-base maintenance[J]. Computational Intelligence: International Journal, 2001, 17(2): 295-314.
[11] YANG Q, ZHU J. A case-addition policy for case-base maintenance[J]. Computational Intelligence: International Journal, 2001, 17(2): 250-262.

(上接第 125页)

且 P_1 是最优的,$N(m-m_0, 2s+1, s, \Gamma; 2(v-m_0)+2)$由式(1)给出。

参考文献:

[1] WAN Zhexian. Further constructions of Cartesian authentication codes from symplectic geometry[J]. Northeastern Math J, 1992, 8(1): 4-20.
[2] 高锁刚. 利用有限域上酉几何构作两类 Cartesian认证码[J]. 高校应用数学学报 A辑(中文版), 1996, (3): 223-234.
[3] YOU H(游宏), GAO Y(高有). Some new construction of Cartesian authentication codes from symplectic geometry[J]. System Sciences and Mathematical Sciences, 1994, 7(4): 317-327.
[4] WAN Zhexian. Geometry of Classical Groups over Finite Fields[M]. Lund: Student-litteratur, 1993.
[5] 童占梅,何 清. 基于分解构造最优模糊等价矩阵的计算[J]. 河北科技大学学报, 1998, 19(2): 59-64.

向本期载文的有关审稿专家致谢

本期《河北科技大学学报》共发表论文 21篇。这些论文的发表,是与有关专家的认真审读、细查资料、推敲分析、中肯评价分不开的。他们的评价(有的给予了充分肯定,有的给出了修改意见,有的指出了存在的问题,有的阐述了否定的原因),使作者和编者都受益匪浅。对此,本刊编辑部特向这些专家表示敬意,对他们的辛勤劳动表示感谢。

本期载文的审稿专家名单如下(按姓名的汉语拼音顺序排序):

陈一鸣 曹玉强 戴松元 董文庚 方志耕 胡 波 孔繁薏 康维钧
李风泉 李国昌 李敏通 李志全 刘明珠 梁普选 仇计清 孙晓云
魏世泽 许克明 郑宝东 翟成波 周卫龙

(本刊编辑部)