数理解析研究所講究録 1440 巻 2005 年 74-81

Relative Difference Sets in Dihedral Groups

Agnes D. Garciano
Mathematics Department, Ateneo de Manila University
Loyola Heights, Quezon City, Philippines

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University
Kurokami, Kumamoto, Japan

Takeo Yokonuma
Department of Mathematics, Sophia University
Kioichi, Chiyoda-ku, Tokyo, Japan

1. Introduction

A (m,n,k,λ) *relative difference set* (RDS) in a finite group G of order mn relative to a subgroup N of order n, is a $k-$element subset R of G wherein every element of $G-N$ has exactly λ representations as $r_1r_2^{-1}$ with $r_1, r_2 \epsilon R$. Moreover, no nonidentity element of N has such a representation. N is called the *forbidden subgroup*. If for a subset X of G, we identify X with the group ring element $X = \sum_{x \epsilon X} x \quad \epsilon \quad \mathbb{C}[G]$ and set $X^{(-1)} = \sum_{x \epsilon X} x^{-1}$, then R is a (m,n,k,λ) RDS in G relative to N if $RR^{(-1)} = k + \lambda(G-N)$. It follows that $k(k-1) = \lambda n(m-1)$. Note that if $N = 1$, then R is an (m,k,λ) difference set in the usual sense.

The notion of a relative difference set was introduced by Elliot and Butson [1]. The following result which is due to them is fundamental in the study of RDS's.

Result 1.1. ([1]) Let R be a (m,n,k,λ) relative difference set in a group G relative to a subgroup N and let U be a normal subgroup of G contained in N. If $\phi : G \to G/U$ is the canonical epimorphism and $|U| = u$, then $\phi(R)$ is a $\left(m, \frac{n}{u}, k, u\lambda\right)$ relative difference set in $\overline{G}(= G/U)$ with respect to $\overline{N}(= N/U)$.

In particular, if $N = U$, then $\phi(R)$ is a $(m,k,n\lambda)$ ordinary difference set in $\overline{G}(= G/N)$. We may then consider R as an "extension" of an ordinary difference set.

Although trivial ordinary difference sets with parameters of the form $(v+2, v+1, v)$ and (v,v,v) , $v > 0$, exist in any group, it is still a question whether or not extensions of these difference sets also exist. In dihedral groups for instance, it is conjectured that only trivial ordinary difference sets exist. Hence, a problem that we would like to consider is whether extensions of these trivial difference sets exist in dihedral groups.

A relative difference set in a group G is said to be *semiregular* or of *affine type* if its parameters are of the form $(n\lambda, n, n\lambda, \lambda)$ or $(n\lambda+2, n, n\lambda+1, \lambda)$ respectively.

If N is a normal subgroup of G and R is either a semiregular or affine type RDS in G, then $\overline{R}$ is a trivial ordinary difference set in $\overline{G}$ by Result 1.1. We say that a (m, n, k, λ) relative difference set is *trivial* if $k = 1$ or $(n, k) \in \{(1, m)\ ,\ (1, m-1)\}$.

If the conjecture mentioned above is true, then the only nontrivial RDS's that can exist in dihedral groups relative to a normal subgroup are either semiregular or of affine type.

The only nontrivial relative difference set up to equivalence in a dihedral group known to the authors is as follows:

Example 1.2. Let $G = \langle x, y \mid x^4 = y^2 = 1\ ,\ y^{-1}xy = x^{-1}\rangle$ be the dihedral group of order 8. Then $D = \{1, xy, x^2y, x^3\}$ is a $(4, 2, 4, 2)$ relative difference set in G relative to $\langle y \rangle$.

In [2], the following was shown.

Result 1.3. ([2]) There exists no nontrivial semiregular relative difference set in any dihedral group relative to a normal subgroup.

In section 3, we prove the following.

Theorem 3.1. There is no relative difference set of affine type in dihedral groups.

2. Preliminaries

We will use the following results which we mention here without proof.

Result 2.1. ([3]) Let X be an $n \times n$ circulant matrix

$$X = \begin{bmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_{n-1} & x_0 & \cdots & x_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ x_1 & x_2 & \cdots & x_0 \end{bmatrix}$$

Then $\det(X) = \prod_{0 \le i \le n-1}(x_0 + \xi^i x_1 + \xi^{2i} x_2 + \cdots + \xi^{(n-1)i} x_{n-1})$, where ξ is a primitive nth root of unity. Moreover, if $\det(x) \neq 0$, then X^{-1} is also circulant.

Result 2.2. ([4]) (Inversion Formula). Let G be an abelian group and $A = \sum_{g \in G} \alpha_g g$ be an element of the group algebra $\mathbb{C}$[G]. Then, $\alpha_g = \dfrac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\, \chi(g^{-1})$ for each $g \in G$ where G^* is the group of characters of G.

Throughout the rest of this paper, we will assume the following:

Assumptions. Let R be a $(n\lambda+2, n, n\lambda+1, \lambda)$ $(\lambda > 0)$ relative difference set in a dihedral group G relative to a subgroup N. Set $G = C\langle t\rangle$ where C is a cyclic group and t is an involution which inverts C. Set $R = A + Bt$ where A and B are subsets of C. By exchanging Rt for R if necessary, we may assume $|A| \leq |B|$.

Proposition 2.3. Under the above assumptions, the following hold:

(i) If $N \subset C$, then $AA^{(-1)} + BB^{(-1)} = (n\lambda+1) + \lambda(C - N)$ and $AB = \dfrac{\lambda}{2}\, C$. Furthermore, $|A| = \dfrac{n\lambda}{2}$ and $|B| = \dfrac{n\lambda}{2} + 1$.

(ii) If $N \not\subset C$, $N_1 = N \cap C$ and $N_2 = Nt \cap C$, then $AA^{(-1)} + BB^{(-1)} = (n\lambda + 1) + \lambda(C - N_1)$ and $AB = \dfrac{\lambda}{2}(C - N_2)$. Furthermore, $|A| = \dfrac{(n\lambda+1) - \sqrt{n\lambda+1}}{2}$ and $|B| = \dfrac{(n\lambda+1) + \sqrt{n\lambda+1}}{2}$.

Proof. We have $RR^{(-1)} = (A + Bt)(A^{(-1)} + tB^{(-1)}) = AA^{(-1)} + BB^{(-1)} + 2ABt$.

Suppose $N \subset C$. By definition, $RR^{(-1)} = (n\lambda+1) + \lambda(C + Ct - N)$. Thus, $AA^{(-1)} + BB^{(-1)} = (n\lambda+1) + \lambda(C - N)$ and $AB = \dfrac{\lambda}{2}\, C$. If $|A| = a$ and $|B| = b$, it follows that $a + b = n\lambda + 1$ and $ab = \dfrac{\lambda}{4}\, n(n\lambda+2)$. Hence (i) holds.

Suppose $N \not\subset C$. Then, $RR^{(-1)} = (n\lambda+1) + \lambda(C + Ct - N_1 - N_2 t)$. Thus, $AA^{(-1)} + BB^{(-1)} = (n\lambda+1) + \lambda(C - N_1)$ and $AB = \dfrac{\lambda}{2}\,(C - N_2)$. If $|A| = a$ and $|B| = b$, it follows that $a + b = n\lambda + 1$ and $ab = \dfrac{\lambda}{4}\, n(n\lambda+2)$. Hence (ii) holds. ∎

3. Nonexistence of Affine Type Relative Difference Sets in Dihedral Groups

To prove our main theorem, we first show a necessary condition on the forbidden subgroup.

Proposition 3.1. Let R be a relative difference set of affine type in a dihedral group G relative to a subgroup N of G. Then, N is normal in G.

We will prove Proposition 3.1 in Lemmas 3.2 - 3.7. As mentioned in the previous section, we let $G = C\langle t\rangle$ where C is a cyclic subgroup of G and t is an element of G which inverts C. Set $R = A + Bt$ where A and B are subsets of C.

Suppose the proposition is false and let G be a minimal counterexample to the proposition. As every element outside C is an involution and inverts C, we may assume that $t \in N$.

Lemma 3.2. $n = 2$. In particular,

(i) $G = CN$, $N = \langle t \rangle$ and $C \cong Z_{2(\lambda+1)}$

(ii) D is a $(2\lambda+2,\ 2,\ 2\lambda+1,\ \lambda)$ relative difference in G with respect to N.

Proof. Let $L = N \cap C$. Then $[N : L] = 2$ and $G \rhd L$ as C is cyclic. Therefore, by Result 1.1, $\overline{D}$ is a difference set with parameters $\left(n\lambda+2,\ 2,\ n\lambda+1,\ \frac{n\lambda}{2}\right)$ in $\overline{G}(= G/L)$ relative to $\overline{N}(= N/L \cong \mathbb{Z})$. Clearly, $\overline{G} \not\rhd \overline{N}$. By the minimality of G, $L = 1$. Thus $N = \langle t \rangle$. ∎

By Proposition 2.3, we have

$$AA^{(-1)} + BB^{(-1)} = (2\lambda+1) + \lambda(C-1) \tag{1}$$

$$AB = \frac{\lambda}{2}\,(C-1) \tag{2}$$

$$|A| = \frac{2\lambda+1-\sqrt{2\lambda+1}}{2} \quad \text{and} \quad |B| = \frac{2\lambda+1+\sqrt{2\lambda+1}}{2} \tag{3}$$

Lemma 3.3. We may assume that $C = A + B^{(-1)} + 1$.

Proof. By (2) and (3), $A \cap B^{(-1)} = \phi$ and $|A| + |B| = |C| - 1$. Hence $C = A \cup B^{(-1)} \cup \{g\}$ for some $g \in C$. Exchanging D for Dg^{-1} if necessary, we may assume that $g = 1$. ∎

Lemma 3.4. $A = A^{(-1)}$ and $B = B^{(-1)}$.

Proof. Let χ be a nonprincipal character of C and set $\chi(A) = a$ and $\chi(B) = b$. By (1), (2) and Lemma 3.3, $a\overline{a} + b\overline{b} = \lambda + 1$, $ab = \frac{-\lambda}{2}$ and $a + \overline{b} + 1 = 0$. It follows that $2a\overline{a} + a + \overline{a} = \lambda = 2a\overline{a} + 2a$. Hence $a = \overline{a}$. By Result 2.2, $A - A^{(-1)} = 0$. Thus, $A = A^{(-1)}$ and as $B = C - A - 1$, we have $B = B^{(-1)}$. ∎

By (3) above, we can set $2s + 1 = \sqrt{2\lambda+1}$ for a positive integer s. Then $\lambda = 2s^2 + 2s$ and D is a $(4s^2 + 4s + 2,\ 2,\ (2s+1)^2,\ 2s^2 + 2)$ RDS in $G(\cong D_{4(2s^2+2s+1)})$. Moreover, by (1), (2) and Lemma 3.4, we have $|A| = 2s^2 + s$, $|B| = 2s^2 + 3s + 1$, $C = A + B + 1$, $A^2 + B^2 = (2s+1)^2 + (2s^2+2)(C-1)$, $AB = (s^2 + s)(C-1)$. Hence, the following hold.

Lemma 3.5. $A^2 + A = s^2C + s^2 + s \quad , \quad B^2 + B = (s+1)^2C + s^2 + s.$

Let M be the unique subgroup of C of index 2 and let d be an involution of C. Then $C = M \times \langle d \rangle$. Set $\overline{C} = C/M (= \{\overline{1}, \overline{d}\})$.

Lemma 3.6. $|A \cap M| = s^2 + s$, $|A \cap Md| = s^2$, $|B \cap M| = s^2 + s$, $|B \cap Md| = (s+1)^2$.

Proof. Let $v = |A \cap M|$ and $w = |A \cap Md|$. Then $\overline{A} = v + w\overline{d}$ and $v + w = |A| = 2s^2 + s$. By Lemma 3.5, $(v + w\overline{d})^2 + (v + w\overline{d}) = s^2(2s^2 + 2s + 1)(\overline{1} + \overline{d}) + s^2 + s$. It follows that $v^2 + w^2 + v = 2s^4 + 2s^3 + 2s^2 + s$ and $2vw + w = 2s^4 + 2s^3 + s^2$ and so $(v-w)^2 + (v-w) = s^2 + s$. Thus, $v - w = s$ or $v - w = -(s+1)$. If $v - w = -(s+1)$, then $2w = 2s^2 + 2s + 1$, a contradiction. Hence $v - w = s$ and so $v = s^2 + s$, $w = s^2$. The other equations in the Lemma can be proven similarly. ∎

Lemma 3.7. s is even.

Proof. By Lemma 3.6, $B \cap Md \neq \phi$. Let $g \in B \cap Md$ and set $\Omega = \{(x, y) \mid x, y \in B, g = xy\}$. By Lemma 3.5, $|\Omega| = (s+1)^2 - 1$. If s is odd, then $|\Omega| \equiv 1 \pmod 2$. As $(x, y) \in \Omega$ implies $(y, x) \in \Omega$, there is an element $z \in B$ such that $(z, z) \in \Omega$. Thus, $g = z^2 \in Md$, a contradiction. Thus, s is even. ∎

Proof of Proposition 3.1:

By Lemma 3.7, $s = 2\ell$ for some integer $\ell > 0$. By Lemma 3.6, $A \cap Md \neq \phi$. Let $g \in A \cap Md$ and set $\Omega = \{(x, y) \mid x, y \in A \text{ , } xy = g\}$. By Lemma 3.5, $|\Omega| = s^2 - 1 \equiv 1 \pmod 2$. By a similar argument as in Lemma 3.7, we have a contradiction. Thus, $G \triangleright N$.

∎

Proposition 3.8. Let G be a dihedral group and N a normal subgroup of G. Then, there is no nontrivial relative difference set of affine type in G relative to N.

In the rest of this section, let G be a minimal counterexample to Proposition 3.8 and let R be a $(p\lambda + 2,\ p,\ p\lambda + 1,\ \lambda)$ RDS in G. By the minimality condition, p is a prime. As mentioned in Section 2, we let $G = C\langle t \rangle$ where t inverts the cyclic group C and let $R = A + Bt$ where A and B are subsets of C. Exchanging R for its translate, if necessary, we may assume $R \cap N = \phi$ and $R \cup \{1\}$ is a complete set of coset representatives of G/N. Since $G \triangleright N$, N is contained in C. By Proposition 2.3, we have

$$AA^{(-1)} + BB^{(-1)} = (p\lambda + 1) + \lambda(C - N) \tag{4}$$

$$AB = \frac{\lambda}{2}\, C \tag{5}$$

$$|A| = \frac{\lambda}{2}\, p \quad , \quad |B| = \frac{\lambda}{2}\, p + 1 \tag{6}$$

Let $h = \frac{\lambda}{2}\, p + 1$. Moreover, let $C = HN$ where $N = \langle s \rangle \cong \mathbb{Z}_p$ and $H \cong \mathbb{Z}_h$. Thus, we can set

$$A = A_0 + A_1 s + \cdots + A_{p-1} s^{p-1}, \quad B = B_0 + B_1 s + \cdots + B_{p-1} s^{p-1} \quad (7)$$

for some subsets A_0 , ... , A_{p-1} , B_0 , ... , B_{p-1} of H.

Lemma 3.9. The following hold:

(i) $A_i \cap A_j = B_i \cap B_j = \phi \quad \forall\, i, j$ with $0 \le i,\ j \le p-1\ ,\ i \ne j$.

(ii) $H = 1 + \sum_{o \le i \le p-1} A_i = \sum_{0 \le i \le p-1} B_i$.

Proof. Since $N = \langle s \rangle$ and $AA^{(-1)} \cap N = BB^{(-1)} \cap N = \{1\}$ by (4), (i) holds. Hence, $|A| = \sum_{0 \le i \le p-1} |A_i|$ and $|B| = \sum_{0 \le i \le p-1} |B_i|$. By (6), $|A| = h - 1$ and $|B| = h$. Then, (ii) follows immediately. ∎

Substituting (7) into equations (4) and (5), we have

$$\begin{aligned}
A_0B_0 + A_1B_{p-1} + A_2B_{p-2} + \cdots + A_{p-1}B_1 &= \frac{\lambda}{2}\, H \\
A_0B_1 + A_1B_0 + A_2B_{p-1} + \cdots + A_{p-1}B_2 &= \frac{\lambda}{2}\, H \\
A_0B_i + A_1B_{i-1} + A_2B_{i-2} + \cdots + A_{p-1}B_{i-p+1} &= \frac{\lambda}{2}\, H \qquad (8)\\
\cdots \ + \ \cdots \ + \ \cdots \ + \ \cdots &= \frac{\lambda}{2}\, H \\
A_0B_{p-1} + A_1B_{p-2} + A_2B_{p-3} + \cdots + A_{p-1}B_0 &= \frac{\lambda}{2}\, H
\end{aligned}$$

and

$$\begin{aligned}
&A_0A_{p-1}^{(-1)} + A_1A_0^{(-1)} + A_2A_1^{(-1)} + \cdots + A_{p-2}A_{p-3}^{(-1)} + A_{p-1}A_{p-2}^{(-1)} \\
&+B_0B_{p-1}^{(-1)} + B_1B_0^{(-1)} + B_2 + B_1^{(-1)} + \cdots + B_{p-1}B_{p-2}^{(-1)} = \lambda(H-1) \quad (9)
\end{aligned}$$

Let χ be a character of H. By (8), we have

$$\begin{bmatrix} \chi(B_0) & \chi(B_{p-1}) & \cdots & \chi(B_1) \\ \chi(B_1) & \chi(B_0) & \cdots & \chi(B_2) \\ \vdots & & \vdots & \\ \chi(B_{p-2}) & \chi(B_{p-3}) & \cdots & \chi(B_{p-1}) \\ \chi(B_{p-1}) & \chi(B_{p-2}) & \cdots & \chi(B_0) \end{bmatrix} \begin{bmatrix} \chi(A_0) \\ \chi(A_1) \\ \vdots \\ \chi(A_{p-2}) \\ \chi(A_{p-1}) \end{bmatrix} = \frac{\lambda}{2}\, \chi(H) \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix} \qquad (10)$$

Lemma 3.10. The following hold.

(i) $|A_0| = |A_1| = \cdots = |A_{p-1}| = \frac{\lambda}{2}$.

(ii) $|B_0||B_{p-1}|+|B_1||B_0|+\cdots+|B_{p-1}||B_{p-2}|=\frac{p\lambda^2}{4}$.

Proof. Let $|A_i|=a_i$ and $|B_i|=b_i$ for $i=0,1,\ldots,p-1$. If χ is the principal character of H, then by (10),

$$\begin{bmatrix} b_0 & b_{p-1} & \cdots & b_1 \\ b_1 & b_0 & \cdots & b_2 \\ \vdots & & & \\ b_{p-2} & b_{p-3} & \cdots & b_{p-1} \\ b_{p-1} & b_{p-2} & \cdots & b_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{p-2} \\ a_{p-1} \end{bmatrix} = \frac{\lambda h}{2} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix} \tag{11}$$

Let P be the $p \times p$ matrix in the above equation (11). By Result 2.1, $\det(P) = \Pi_{0\le i\le p-1}(b_0+b_{p-1}\zeta^i+b_{p-2}\zeta^{2i}+\cdots+b_1\zeta^{(p-1)i})$, where ζ is a primitive p–th root of unity. By Lemma 3.9 (ii), $b_0+b_{p-1}+b_{p-2}+\cdots+b_1=|H|\neq 0$. Suppose $b_0+b_{p-1}\zeta^i+b_{p-2}\zeta^{2i}+\cdots+b_1\zeta^{(p-1)i}=0$ for some $i\neq 0$. Set $\theta=\zeta^i$. Then, θ is a primitive p–th root of unity and $x^{p-1}+x^{p-2}+\cdots+x+1$ is a minimal polynomial of θ over $\mathbb{Q}$. Hence $b_0=b_{p-1}=b_{p-2}=\cdots=b_1$. However, $pb_0=\sum_{0\le i\le p-1} b_i=|H|=\frac{\lambda}{2}p+1$, a contradiction. Thus $\det(P)\neq 0$. By Result 2.1, P^{-1} is also circulant. Since $(a_0,a_1,\ldots,a_{p-1})^T=\frac{\lambda h}{2}\ P^{-1}(1,1,\ldots 1)^T$, it follows that $a_0=a_1=\cdots=a_{p-1}$. Hence, by Lemma 3.9, $a_0=a_1=\cdots=a_{p-1}=\frac{\lambda}{2}$. Thus (i) holds and (ii) follows from (9) and (i).

Lemma 3.11. Let χ be a non-principal character of H. Then $\chi(B_0)=\chi(B_1)=\cdots=\chi(B_{p-1})=0$.

Proof. Set $\chi(A_i)=\alpha_i$ and $\chi(B_i)=\beta_i$ for $i=0,1,\ldots,p-1$. By (10)

$$\begin{bmatrix} \alpha_0 & \alpha_{p-1} & \cdots & \alpha_1 \\ \alpha_1 & \alpha_0 & \cdots & \alpha_2 \\ \vdots & & & \\ \alpha_{p-2} & \alpha_{p-3} & \cdots & \alpha_{p-1} \\ \alpha_{p-1} & \alpha_{p-2} & \cdots & \alpha_0 \end{bmatrix} \begin{bmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{p-2} \\ \beta_{p-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} \tag{12}$$

Let Q be the $p \times p$ matrix in the equation (12) above. By Result 2.1, $\det(Q)=\Pi_{0\le i\le p-1}(\alpha_0+\alpha_{p-1}^{\zeta^i}+\alpha_{p-2}\zeta^{2i}+\cdots+\alpha_1\zeta^{(p-1)i})$, where ζ is a primitive pth root of unity. Let $i\neq 0$, $i\in\{0,1,\ldots,p-1\}$ and let $\eta=\alpha_0+\alpha_{p-1}\theta+\alpha_{p-2}\theta^2+\cdots+\alpha_1\theta^{p-1}$ where $\theta=\zeta^i$. Then, we have $\eta^p=\alpha_0^p+\alpha_{p-1}^p+\alpha_{p-2}^p+\cdots+\alpha_1^p \pmod p \equiv \sum_{0\le i\le p-1}\left(\sum_{x\in A_i}\chi(x)\right)^p \pmod p \equiv \sum_{0\le i\le p-1}\left(\sum_{x\in A_i}\chi(x^p)\right) = \sum_{x\in\{A_0,\ldots,A_{p-1}\}}\chi(X^{(p)}) = \chi(H^{(p)}-1)$ by Lemma 3.9 (ii). On the other hand, $H^{(p)}=H$ as $(p,h)=1$. Hence $\eta^p\equiv -1$

(mod p) and so $\eta^p = -1 + p\alpha$ for an algebraic integer $\alpha \in \mathbb{Z}[\theta]$. If $\eta = 0$, then $\alpha = \frac{1}{p}$, a contradiction. Hence $\det(Q) \neq 0$. Thus, the lemma holds.

Proof of Proposition 3.8:

By Lemma 3.11 and Result 2.2, there exist $c_0, c_1, \ldots, c_{p-1} \in \mathbb{C}$ such that $B_0 = c_0H, B_1 = c_1H, \ldots, B_{p-1} = c_{p-1}H$. Since each B_i is a subset of H , $B_{i_0} = H$ and $B_i = \phi(\forall i \neq i_0)$ for some $i_0 \in \{0, 1, \ldots, p-1\}$. By Lemma 3.10, $\frac{p\lambda^2}{4} = 0$. Thus $\lambda = 0$, a contradiction. ∎

By Propositions 3.1 and 3.8, we have the following.

Theorem 3.12. There is no nontrivial relative difference set of affine type in dihedral groups.

References

[1] J.E. Elliot and A.T. Butson, Relative difference sets, *Illinois J. Math.* vol 10 (1966), pp. 517 - 531.

[2] D.T. Elvira and Y. Hiramine, On Non-Abelian Semi-Regular Relative Difference Sets, *Finite Fields and Applications*, Springer, Berlin, 2001, pp. 122 - 127.

[3] W. Greub, *Linear Algebra*, fourth edition, Springer, (1975).

[4] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995).