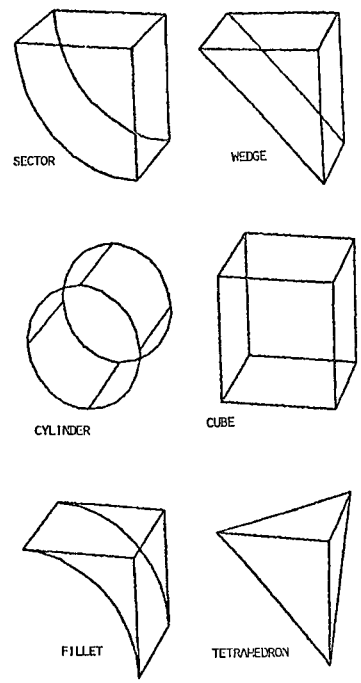
Fig. 8. Primitive objects.



build it, themselves an alternative description, accupied 300 words. The program is fully described in [2].

4. Conclusion

The main result of this work is that objects bounded by many mathematically simple faces are easily built up by adding and subtracting simpler objects. Efficient algorithms can be devised to carry out addition and subtracting if the operations are restricted in certain respects. Even with these restrictions and surfaces limited to planes and parts of cylinders, the variety of objects which can be made covers a good proportion of the machined components found in practice. The simple command language used to drive the program seems adequate for engineering designers, though an algorithmic language might also be employed. The latter approach has been followed in the EUKLID system [3].

Acknowledgments. The author wishes to thank C.A. Lang and A.R. Grayer of the CAD Group, Computer Laboratory, Cambridge, whose interest and suggestions have greatly benefited this work.

Received February 1974; revised July 1974

References

1. Bellman, R., et al. Abstraction and pattern classification. *J. Math. Anal. and Applications 13* (1966), 1–7.
2. Braid, I.C. *Designing with Volumes* (2nd ed.). Cantab Press, 97 Hurst Park Ave, Cambridge, U.K., 1974.
3. Engeli, M., and Hrdliczka, V. *EUKLID-eine Einfiihrung.* Fides Rechenzentrum, Zurich, 1974.
4. Lang, C.A. SAL—systems assembly language. Proc. AFIPS 1969 SJCC. Vol. 38, pp. 543–555, AFIPS Press, Montvale, N.J.
5. Newman, W.M., and Sproull, R.F. *Principles of Interactive Computer Graphics.* McGraw-Hill, New York, 1973.

Programming Techniques

G. Manacher Editor

The Quadratic Hash Method When the Table Size Is Not a Prime Number

Vladimir Batagelj
"Jožef Stefan" Institute,
University of Ljubljana

Previous work on quadratic hash methods is limited mainly to the case where the table size is a prime number. Here, certain results are derived for composite numbers. It is shown that all composite numbers containing at least the square of one of the component primes have full-period integer-coefficient quadratic hash functions.

Key Words and Phrases: quadratic search, hash code, scatter storage, table size

CR Categories: 3.74, 4.10

From the literature one gains the impression that the period of quadratic search is usually too small for effective use when the table size is not a prime number [1]. For this reason, most authors limit themselves to quadratic methods for tables whose size is a prime number or a special prime power. For example, the sequence $z_i \equiv z_o + Ri + \frac{1}{2}i(i+1) \pmod{2^k}$ due to Hopgood and Davenport [2] has the period of search $2^k - R$. The coefficient $\frac{1}{2}$ is not an integer, which underlies the belief that integer-coefficient full-period quadratic hash functions may be rare or nonexistent. However, this belief, as we shall now show, is false.

Consider the sequence

$$z_i \equiv z_0 + ai + bi^2 \pmod{d} \qquad (1)$$

for $i = 0, 1, 2, \ldots$ where a and b are integer constants and d is the table size. We reduce the problem of the period of search to the question whether there exist in-

Author's address: "Jožef Stefan" Institute, Jamova 39, 61 001, Ljubljana p.p. 199, Yugoslavia.

dices i and j such that

$$z_i = z_j \quad \text{and} \quad 0 \leq i < j < d. \tag{2}$$

That is equivalent to

$$z_j - z_i \equiv (j - i)(a + b(i + j)) \equiv 0 \pmod{d}. \tag{3}$$

When d is a prime number, it is known [1, 3, 4] that the sequence (z_i) examines one half of the table (each entry twice) in the first d steps. This is due to the fact that the set of residues modulo a prime number is a field. In particular, in a field the equation $a + bx \equiv 0 \pmod{d}$ has exactly one solution for any a and b ($b \not\equiv 0$). If besides this $a \equiv 0 \pmod{d}$ or $a \equiv b \pmod{d}$ the sequence (z_i) examines one half of the table already in the first $(d + 1)/2$ steps.

For primes of the form $4k + 3$, we can construct a "quadratic" sequence which examines the whole table in the first d steps [3], [5].

The existence of a solution of eq. (3) is what we wish to avoid. If we can find the coefficients a and b for which there do not exist integers i and j which at the same time satisfy condition (2) and eq. (3), then the corresponding sequence (z_i) has the period of search d.

Let d take the form

$d = \prod_{i \in I} p_i^{\alpha_i}$ where p_i are prime numbers, and for some $i \in I : \alpha_i > 1$. If $B = \prod_{i \in I} p_i$

and A satisfies the condition $(A,B) = 1$, then the sequence (z_i) with $a = A$ and $b = BC$ (C any integer) examines the whole table in the first d steps.

The proof is trivial. Evidently $c = a + b(i + j) = A + BC(i + j)$ is coprime with d; we write $(c,d) = 1$.

For this reason we can divide eq. (3) by c. We get an equivalent equation $j - i \equiv 0 \pmod{d}$ which has no solution under condition (2).

Coefficients A and C can be used to reduce secondary clustering [6]. If $BC \equiv 0 \pmod{d}$, this method reduces to the linear one proposed by Bell and Kaman [7]. The special case of this theorem for $d = p^n$, $n > 1$ was found independently by Frank Ackerman [9].

Example 1

$d = 2^k, \quad k > 1$

$z_i \equiv z_0 + (2Q + 1)i + 2Ri^2 \pmod{2^k}$

for any integer Q and R.

Example 2

$d = 10^k, \quad k > 1$

$z_i \equiv z_0 + Qi + 10Ri^2 \pmod{10^k}$

Q and R are integers; Q must be an odd number whose last digit is not equal to 5.

This can be extended to polynomials of higher degrees straightforwardly, i.e. let

$$z_i \equiv z_0 + \sum_{k=1}^{n} a_k i^k \pmod{d},$$

$(a_1, B) = 1$, and for every k, $2 \leq k \leq n$; $z_k \equiv Bb_k$. Then the sequence (z_i) has period d.

Recently, Franc Dacar of the Ljubljana University Computing Center has found necessary and sufficient conditions for integer-coefficient quadratic hash function to have full period [8]. He has found that hash function has period d if and only if the conditions from the theorem are fufilled or the following conditions hold:

(1) $d = 2d_1$, where d_1 is odd.

(2) $a = 2a_1$, $(a_1, d_1) = 1$.

(3) b is odd and all primes dividing d_1 also divide b.

If d_1 is a product of different primes, then $\Delta z_i \equiv d_1 + a \pmod{d}$ and consequently the sequence (z_i) is linear.

From this result we can see that a necessary and sufficient condition on d for existence of full-period quadratic search is either that the factorization of d contain at least one prime power or that d be two times the product of distinct odd primes.

The quadratic method is usually realized by the following difference schema modulo d:

$\Delta^2 z_i \equiv b, \Delta z_0 \equiv a, \Delta z_{i+1} \equiv \Delta z_i + \Delta^2 z_i, z_{i+1} \equiv z_i + \Delta z_i$

that determines the sequence

$$z_i \equiv z_0 + ai + b\binom{i}{2} \pmod{d}.$$

If b is even, the hash function has integer coefficients. For odd b it turns out that only sequences of the form

$$z_i \equiv z_0 + b\binom{i+1}{2} \pmod{2^k}$$

have the full period.

A detailed theory of quadratic hash functions (based on [8]) will be described in a separate paper.

Acknowledgments. I am grateful to Glenn K. Manacher, editor for Programming Techniques and to Dr. Boštjan Vilfan from "Jožef Stefan" Institute for suggesting some improvements in exposition and content.

Received December 1973; revised August 1974

References

1. Maurer, W.D. An improved hash code for scatter storage. *Comm. ACM 11*, 1 (Jan. 1968), 35–38.
2. Hopgood, F.R.A., and Davenport, J. The quadratic hash method when the table size is a power of 2. *Comput. J. 15*, 4 (1972), 314–315.
3. Radke, Charles E. The use of quadratic residue research. *Comm. ACM 13*, 2 (Feb. 1970), 103–105.
4. Lamport, Leslie Comment on Bell's quadratic quotient method for hash code searching. *Comm. ACM 13*, 9 (Sept. 1970), 573–574.
5. Day, A. Colin Full table quadratic searching for scatter storage. *Comm. ACM 13*, 8 (Aug. 1970), 481–482.
6. Bell, James R. The quadratic quotient method: A hash code eliminating secondary clustering. *Comm. ACM 13*, 2 (Feb. 1970). 107–109.
7. Bell, James R., and Kaman, Charles H. The linear quotient hash code. *Comm. ACM 13*, 11 (Nov. 1970), 675–677.
8. Dacar, F. Range and structure of quadratic sequences (unpublished). Ljubljana U. Computing Center, Ljubljana, 1974.
9. Ackerman, F. Quadratic search for hash tables of size p^n. *Comm. ACM 17*, 3 (Mar. 1974), 164.